Tp Réseaux

Année 2010 -2011

IUT R&T, Nice Sophia-Antipolis

Énoncés

Contributeurs : Thomas André, Luc Deneire, Anwar El Hamra, Rares Serban, Jean Gourdin (Académie de Créteil), Philippe Latu, Franck Maucci, Laurent Kwiatkowski, Lucile Sassatelli

Document sous licence GPL : Permission vous est donnée de copier, distribuer et/ou modifier ces documents selon les termes de la licence GNU Free Documentation licence, Version 1.1 ou ultérieur publiée par la Free Software Foundation ». Pour plus d'informations, voir le texte de la licence à http://www.gnu.org/licenses/fdl.html

Préambule

Le module de Tps « réseau » aborde principalement l'installation et la surveillance des réseaux locaux de type ethernet. La première partie (deux Tps) consiste en une introduction au câblage. La deuxième partie consiste en un TP de simulation d'Ethernet, avec comme objectif de vous faire découvrir les architectures simples que vous pourrez rencontrer et l'influence de choix simples sur la performance du réseau. La troisième partie (et la plus importante) vous introduira à la surveillance (l'audit) de réseau via une sonde et via un programme de surveillance. L'intérêt est principalement de vous donner l'occasion d'explorer les réseaux ethernet et de vous confronter avec les rudiments de l'installation et la la surveillance de ces systèmes. Dans ce cadre, il est **IMPORTANTISSIME** de lire les documents fournis **AVANT** de venir en TP.

Déroulement

De manière à permettre à tous les TP de se faire sans dupliquer le matériel inutilement, tout en permettant de faire les TP dans un ordre logique, l'organisation des TPs se fait selon le tableau ci-dessous, avec chaque colonne représentant les TP faits à la séance correspondante, et les lignes les TP en fonction de votre numéro de binôme.

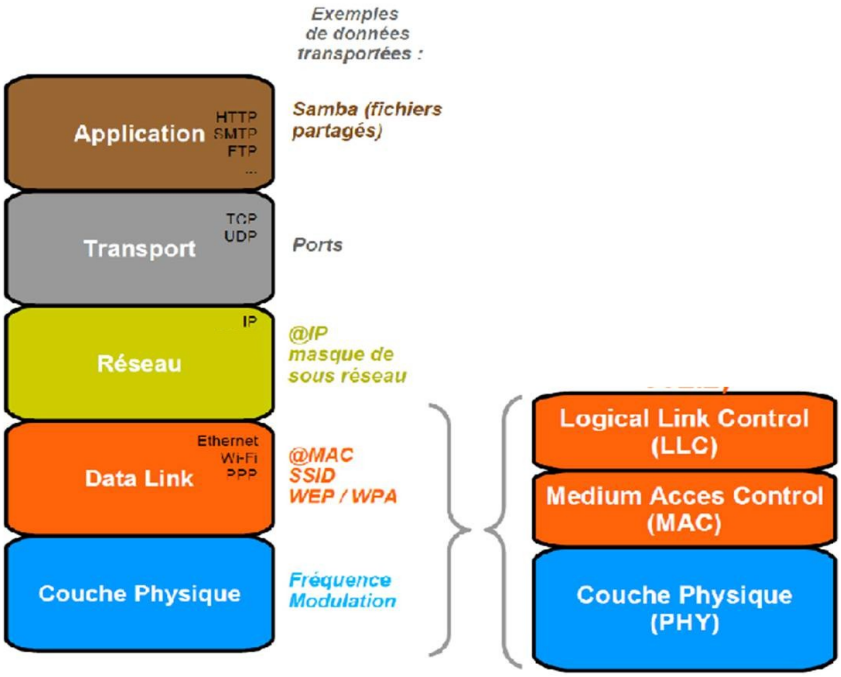
	S1	**S2**	**S3**	**S4**	**S5**	**S6**	**S7**
Binôme 1	Câblage 1	Rmon 1	Rmon 2	Wireshark 1	Wireshark 2	Opnet simu	Câblage 2
Binôme 2	Câblage 2	Câblage 1	Rmon 1	Rmon 2	Wireshark 1	Wireshark 2	Opnet simu
Binôme 3	Opnet simu	Câblage 2	Câblage 1	Rmon 1	Rmon 2	Wireshark 1	Wireshark 2
Binôme 4	Wireshark 1	Opnet simu	Câblage 2	Câblage 1	Rmon 1	Rmon 2	Wireshark 2
Binôme 5	Wireshark 1	Wireshark 2	Opnet simu	Câblage 2	Câblage 1	Rmon 1	Rmon 2
Binôme 6	Rmon 1	Wireshark 1	Wireshark 2	Opnet simu	Câblage 2	Câblage 1	Rmon 2

Consignes à lire en début de chaque TP : Procédure et notation

- **Notation** : La note de TP de R4 est constituée d'une note de contrôle continu = note rapport + interrogation en séance, et d'une note de DS de TP (en dernière semaine). Vous rendez un rapport par binôme à la fin de chaque séance de 3h.
- **Rapport** : A chaque question des sujets de TP qui ne sont pas des instructions de manipulation directe, vous devez répondre dans le rapport. Les réponses doivent toujours établir un lien avec le cours. Notamment, l'**interprétation en terme de couche OSI est capitale**. N'hésitez pas à faire des schémas (de topologie ou autre) dans le rapport pour qu'il gagne en clarté.
- **Notation en séance** : Si une partie de manipulation doit être validée, appelez l'enseignant pour la vérifier.
- **Conseils** :
  - Devant une installation (notamment pour les TP de câblage), il faut comprendre cette installation et ne pas la considérer comme une boîte noire. N'hésitez pas à vous contorsionner pour voir les branchements. N'hésitez donc pas à regarder de partout. En revanche, **ne touchez surtout pas ce qui n'est pas sensé être manipulé par vous** ! (Les dégradations sont rapides avec le nombre d'élèves.)
  - Lorsqu'on vous demande de tester une connexion, ne vous précipitez pas sur un navigateur web. Ayez conscience des mécanismes sous-jacents du réseau que vous avez appris en cours cette année : vous savez que la connexion au réseau local peut

fonctionner sans que vous soyez relier ou que vous ayez le droit de sortir du réseau local. Un test de connexion se fait donc sur le réseau local, par exemple par un ping vers le serveur de la salle (cf configuration de la salle ci-dessous).

- Vous devez venir en TP avec vos cours de réseau (R1, R2, R3, et R4). Dans tous les TP vous avez un accès web. Vous pouvez donc vous munir des versions électroniques des cours où y accéder en ligne.
- N'hésitez pas à chercher des informations en autonomie sur le web. NB: tout copier-coller de wikipedia sera remarqué...
- Les TP ne peuvent se faire indépendamment du cours, ils sont son application. Vous ne pourrez donc pas profiter (et accessoirement avoir une bonne note) des TP si vous venez en séances sans connaître votre cours.
- Les couches OSI doivent être parfaitement comprises et apprises. Un rappel ci-dessous.

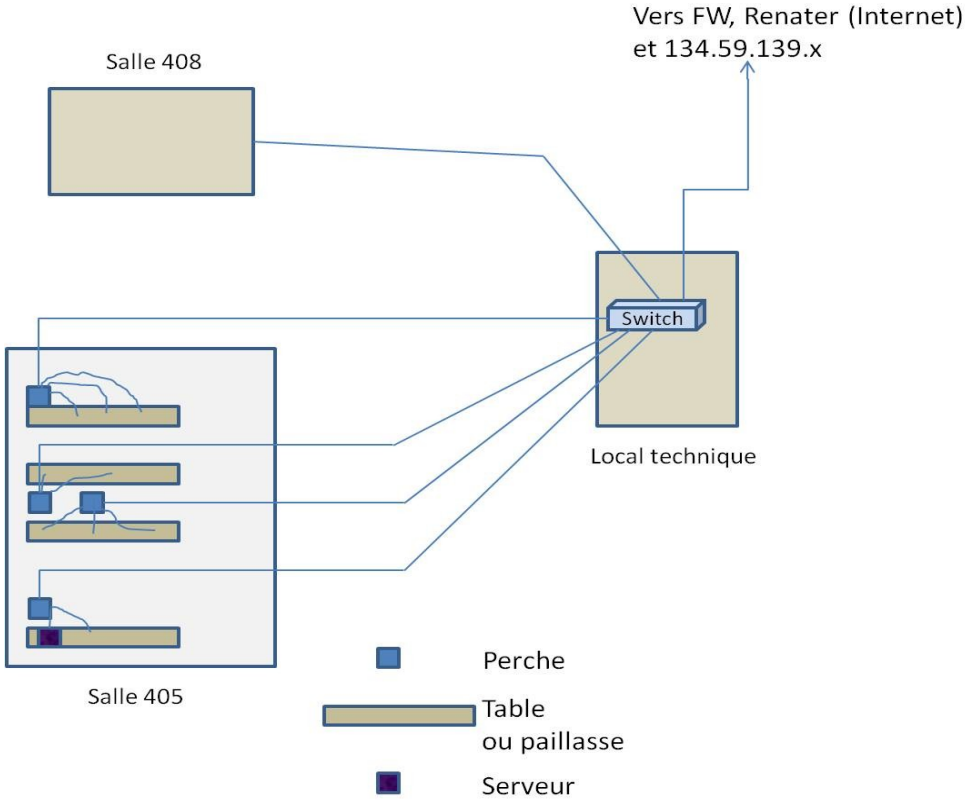


Configuration réseau de la salle

Chaque salle du 4ème étage du bâtiment RT correspond à un réseau local particulier, dont l'adresse réseau est 10.4.1x.0 /24 . Le x vaut 05, 08 ou autre selon qu'on est en 405, 408. Dans notre cas, le réseau local est donc 10.4.105.x/24. Chaque réseau local correspond en fait à un VLAN (Virtual LAN) : ceci signifie que tous ces réseaux sont en fait reliés à un même switch, situé dans le local entre la salle 404 et le bureau 401. Ce switch effectue une segmentation en différents réseaux selon ses ports. Ce switch dispose également d'une connexion vers l'extérieur, notamment vers le réseau de l'IUT RT qui est en 134.59.139.x. Un firewall se trouve en sortie des réseaux 10.4.1x.0. Cela signifie donc que toutes (ou presque) les prises murales de la salle 405, situées sur les perches de chaque tables, sont reliés par des câbles partant dans le faux plafond au switch de l'autre côté du couloir.
Sur le réseau 10.4.105.x, se trouvent 2 machines très importantes:

- la **passerelle** du réseau vers l'extérieur, c'est-à-dire le routeur dont un port est connecté au réseau local 10.4.105.x, et qui permet d'assurer le lien vers les autres réseaux. L'adresse de la passerelle (c'est-à-dire l'adresse IP de l'interface de ce routeur pour ce port) est **10.4.105.254**. Le routeur ne se trouve pas dans la salle 404.

- le **serveur** de la salle 405, qui est la machine du fond de la salle, non accessible aux étudiants. Ce serveur est un serveur DNS, un serveur DHCP, un serveur mail et un serveur d'impression. Son adresse est **10.4.105.253**. Pour testez vos connexions, vous pourrez faire des ping vers ce serveur.



Configuration système de la salle

TP1 :	Pour les 3 PC Linux: login/pwd est *etudiant/etudiant*
TP2:	Pour le PC Linux (le blanc) : *etudiant/Etudiant007*
TP3:	PC Windows, pas de mot de passe
TP4 et 5 :	les TP Wireshark se font sur machine virtuelles Linux. Machine hôte (Ubuntu) : *UserRT/UserRT*. Machine virtuelle: *user/user*. Mot de passe root : *root*.
TP6:	PC windows pas de pwd
TP7:	Machine virtuelle windows pas de pwd

TP 1 - Câblage : équipements d'interconnexion et segmentation

Introduction

L'objectif est de se familiariser avec les techniques de câblage réseau, les équipements d'interconnexion et les principes de segmentation d'un réseau. Après avoir étudié le réseau de la salle de TP (cf. début du fascicule de TP), vous devrez mettre sur le réseau l'ordinateur puis sécuriser ce réseau en segmentant celui-ci avec un switch.

Les ensembles de prises dans l'armoire sont des modules de raccordement de la gamme RCP (raccordements cuivre) utilisés à des points de concentration, comme dans un répartiteur général, sous répartiteur, point de consolidation, etc. Leur technologie leur offre la possibilité de supporter l'ensemble des applications les plus couramment utilisées telle que la voix, la donnée et l'image (VDI), utilisant généralement des câbles de catégorie 6. Les interconnexion sont ainsi plus fiables que des RJ45, engendrant moins d'erreurs, et plus pratiques à administrer.

Des câbles bleus sont à votre disposition en haut de l'armoire pour effectuer toutes les connexions demandées dans la suite. Ce sont des câbles Ethernet avec connecteurs CBE s'enfichant dans les prises RCP. Tout est donc équivalent à du RJ45, mais pas sous le format jack RJ45.

NB: Les câbles bleus sont à manier avec précaution, attention lors du branchement, il y a des détrompeurs sur les câbles, ne forcez pas ! Tous les câbles sont droits (vous aurez à expliquer pourquoi cela suffit dans les questions suivantes).

EN AUCUN CAS VOUS NE DEVEZ TOUCHER AUX CONNEXIONS DES PC AUX PRISES DE LA TABLE

Questions

Partie 0 : Prise en main

Prenez le temps d'identifier la configuration pour ce TP:

- identifier quels sont les équipements d'interconnexion présents dans l'armoire
- repérer toutes les étiquettes dans l'armoire, indiquant la façon dont est faite la partie de câblage non facilement visible
- identifier chacun des ensembles de prises de l'armoire : quels sont les connexions avec les équipements précédents ? Avec les PC ?
- identifier les alimentations en réseaux sur la perche située derrière l'armoire de brassage
- identifier leurs arrivées au niveau de l'armoire

Partie 1 : Premiers tests avec le hub

Dans un premier temps, on veut établir la connexion depuis la perche vers le Hub :

- quel type de câble (droit ou croisé) faudrait-il normalement utiliser, connaissant la topologie du réseau de la salle (donnée en début du fascicule de TP) ?
- Pourquoi ? Rappeler les ensembles MDI/MDIX
- En observant le hub, indiquer comment un câble droit peut convenir.
- Etablir la connexion perche / hub.

- Connectez PC1 sur le hub via les points d'accès appropriés.

- Vérifiez la réussite de votre manipulation (cf. début du fascicule: protocole de test d'une connexion).
- Comment récupérer l'adresse IP et l'adresse MAC de votre machine : En Windows ? En Linux ?
- Comment déterminer l'adresse MAC d'un équipement à partir de son adresse IP ? Décrivez pour cela l'envoi d'un ping avec le mécanisme ARP.
- Relevez les adresses IP et MAC de PC1, ainsi que celles des machines dont vous connaissez les adresses en connaissant la configuration du réseau de la salle.

Partie 2 : Premiers tests avec le switch

Alimentez le switch directement en Internet en reliant le câble venant de la perche sur le switch (en port 9 par exemple) et reliez les 4 ordinateurs à votre disposition sur les ports 1 à 4 du switch.

- Vérifiez la réussite de votre manipulation sur chacun. Pensez à vérifier la configuration de l'interface réseau, et désactiver et ré-activer les interfaces si les premiers tests n'aboutissent pas.

Partie 3 : Installation du switch et accès en mode console

Munissez-vous du guide d'utilisation du switch (posé à votre portée) pour comprendre et répondre aux questions suivantes.

Trois interfaces sont disponibles pour le switch. Le mode *console* permet de se brancher directement sur le switch par port série et d'obtenir une émulation de type VT-100. Le mode *telnet* permet d'accéder au même genre de menu de configuration, mais en utilisant le protocole Telnet au dessus d'une connexion TCP/IP. Enfin, le mode *interface de navigateur Web* (ou *Web browser interface*) permet d'accéder à la configuration et supervision du switch via une connexion HTTP (pages html). Néanmoins, ces deux derniers modes d'accès nécessitent une connexion TCP/IP, et requièrent donc que le switch dispose d'une adresse IP, ce qui n'est pas le cas s'il n'a pas été configuré pour. Il va donc falloir utiliser la connexion série pour ensuite pour avoir accéder au switch par le réseau. Le port série du switch est relié au port série du PC qui jouxte l'armoire.

- D'abord, pour assurer une configuration stable, faire un *reboot d'usine* (cf. notice d'utilisation du switch).
- Dans un terminal du PC, lancer le communicateur série `hyperterminal`.
- Configurez une nouvelle connexion série vers le switch. Les paramètres de cette connexion doivent être trouvés dans la notice du switch. Indiquez-les dans votre rapport.
- Taper deux fois sur la touche `Entrée`. Si tout se passe bien, vous entrez alors dans le menu de configuration du switch en mode console.
- Lorsque hyperterminal établit la connexion avec le switch en mode console, une page d'accueil apparaît puis un prompt CLI. A ce prompt, tapez « menu ».
- Quels sont les avantages et inconvénients de pouvoir supprimer les mots de passe par simple pression d'un bouton à l'avant du switch ?

Note (mots de passe) : Dans le cas où un mot de passe serait requis pour entrer dans le mode console, il peut être effacé par une pression sur le bouton `Clear` à l'avant du switch. Cette

opération réinitialise toutes les protections par mot de passe de la configuration du switch.

Note (retour à la configuration d'usine) : Le retour à la configuration « d'usine » se fait par une pression simultanée sur les boutons `Reset` et `Clear`, en gardant appuyé ce dernier jusqu'à ce que le voyant *Self Test* commence à clignoter.
On peut également, dans le mode CLI , taper la commande `erase startup-config` pour faire rebooter le switch dans sa configuration d'usine.

Partie 4: Attribution d'une adresse IP

Dès que le switch disposera d'une adresse IP, l'accès au mode console sera également accessible par un simple `telnet`. Par défaut, le switch est configuré pour acquérir une adresse IP par DHCP/Bootp. Il peut également être forcé en mode manuel pour recevoir une adresse IP spécifique.

1. Depuis le menu principal, aller dans `2. Switch Management Access Configuration` puis `1. IP Configuration,` faire ensuite l'action `Edit`, se déplacer sur `IP Config [DHCP/Bootp]:` et appuyer sur la touche espace pour positionner `Manual`.
2. Donner ensuite l'adresse IP `10.4.105.41` avec le masque de réseau `255.255.255.0`. La passerelle sera en `10.4.105.254.` Faire alors l'action `Save`: le switch dispose d'une adresse IP.
3. Dans le menu `3. Switch Configuration` puis `1. System Information` pour les 2424M, il est possible de donner un nom au switch (pour faciliter son identification: par exemple, *SwitchN* comme dans la figure plus bas).

- Quel est la couche OSI concernée par le travail d'un switch ?
- Quelle est la couche OSI correspondant à IP ?
- Expliquer alors pourquoi nous attribuons une adresse IP à nos switchs.
- A quoi faut-il faire attention lors de l'attribution de l'adresse IP au switch ?

Partie 5 : Accès au switch sans liaison série

Puisque le switch dispose d'une adresse IP, il est possible de s'y connecter en mode console par un `telnet` ou bien en mode navigateur par HTTP. Néanmoins, soyez conscients du fait que seul le mode console (liaison série) ne *pollue* pas les observations que l'on peut faire sur le trafic: les modes telnet ou Web étant supportés par TCP/IP, et donc transportés par Ethernet, ils génèrent des trames Ethernet qui peuvent rendre confuses les observations que vous devez réaliser dans la suite de ce TP.

1. Donnez à la carte réseau des PC numéro x (`eth0`), l'adresse `10.4.105.1x0`. Pour cela, vérifier par `ifconfig eth0 down` que l'interface `eth0` est bien "tombée", puis remontez la avec une ligne de commande de la forme:
   `ifconfig eth0 10.4.105.1x0 netmask 255.255.255.0 up`
2. Tentez un `ping` vers l'adresse IP que vous avez donnée au switch.
3. Le logiciel `wireshark` permet d'observer le trafic dans un mode graphique. Lancez Wireshark.
4. Une fois que le switch et le PC sont visibles l'un de l'autre, accédez au switch en mode telnet.

5. Regarder ses tables d'adressage ainsi que l'état de ses ports.
6. Qu'est-ce qu'une table d'adressage ?
7. Faire la même chose en accédant au switch via l'interface Web par l'URL `http://10.4.105.41` et regardez les différents onglets (constatez avec `wireshark` les répercutions sur le trafic).

- Décrivez les avantages et inconvénients de chacun des modes d'accès aux switchs (console, telnet et Web).
- Pouvez-vous voir la table d'adressage et l'état des ports du switch dans tous les modes ?
- A quoi correspond la table d'adressage ?

Partie 6: Établissement de la table d'adressage du switch et tables ARP des machines

Pour étudier la commutation Ethernet, nous utilisons un outil relativement simple: `ping`. Néanmoins, même s'il est simple et permet de générer des trames Ethernet, cet outil travaille au niveau 3 des couches OSI, c'est-à-dire au niveau IP (le message ICMP echo request est encapsulé par IP).

L'état de la table ARP peut être consulté sur A avec la commande `arp -a`. Il ne faut pas confondre cette table ARP (@MAC<=>@IP) avec la table des adresses (@MAC<=>n°port) du switch.

Etude de l'établissement de la table ARP d'un PC :

1. Sur PC1, connectez-vous au switch en mode série et affichez la table d'adressage.
2. Sur PC2 et PC4, lancez wireshark.
3. Sur PC3, effacez le contenu de la table arp en faisant arp -a et en faisant arp -d @IP pour l'adresses IP de PC4 si elle s'y trouve.
4. Lancez une capture sur PC2 et PC4.
5. De PC3, faire un ping vers PC4.
6. Des paquets visibles (à analyser) sur PC2 et PC4, que déduisez-vous comme mécanisme d'établissement de la table ARP d'un PC ?

Etude de l'établissement de la table d'adressage du switch :

7. Sur PC1, connectez-vous au switch en mode série et affichez la table d'adressage.
8. Sur PC2, lancez wireshark..
9. Débranchez et rebranchez les ports des PC3 et PC4 sur le switch, et vérifier que ces entrées disparaissent de la table d'adressage.
10. Lancez une capture sur PC2.
11. De PC3, faire un ping vers PC4. Simultanément regardez l'évolution de la table d'adressage du switch (sur PC1).
12. Des paquets visibles (à analyser) sur PC2, que déduisez-vous comme mécanisme d'établissement de la table d'adressage d'un switch ?

Partie 7 : Port Monitoring

Pour surveiller le trafic, il est possible de renvoyer sur un port précis du switch la totalité du trafic qui circule normalement sur un ou plusieurs autres ports. Cela peut être particulièrement intéressant pour surveiller l'activité d'un ensemble de ports.

1. Configurez le switch de façon à ce que le port 4 du switch reçoive les trafics des ports 2 et 3 du switch (4 est dit *moniteur*). Ceci est réalisé en interne, sans câble extérieur. Pour cela, dans le menu principal, faire `Switch Configuration` puis `Network Monitoring Port` et placer `Monitoring Enabled` à `Yes`. Spécifier ensuite qui est moniteur et qui est monitoré.
2. Observer depuis le PC4 (avec `wireshark`), l'activité sur les ports monitorés au repos et lors de ping entre différentes machines : que constatez-vous ?

Partie 8 : Domaines de diffusion

Dans cette partie, vous allez configurer deux VLAN par port, un « rouge » et un « vert ». Chaque VLAN comprendra deux machines.

1. Vérifier l'état de la table d'adressage du switch et regarder le trafic sur chacune des interfaces des PC (avec `wireshark`), en particulier lors de ping entre les différents PC.
2. En l'absence de toute information dans la table d'adressage du switch, vérifier que tous les PC voient les messages ICMP générés par un ping, y compris les trames unicast.
3. Vérifiez que lorsque le switch dispose de l'association, seules les deux machines concernées par le ping voient le trafic. Que se passe-t-il alors si la machine réalisant le ping n'a plus rien dans sa table ARP ?

VLANs non taggés

On désire maintenant que le trafic entre PC1 et PC4 soit complètement différencié du trafic entre PC2 et PC3, c'est à dire qu'aucun échange ni observation ne puisse avoir lieu entre ces deux *réseaux locaux virtuels*. Pour cela, on peut créer deux VLANs distincts: le VLAN *rouge* pour PC1 et PC4 et le VLAN *vert* pour PC2 et PC3. Ce sont des VLANs *par port*, compatibles avec la norme IEEE 802.1Q. En l'absence de toute configuration, les switchs considèrent que tous les ports font partie du même VLAN par défaut.

1. Autoriser les VLANs
   Dans le menu principal d'administration du switch, aller dans `Switch Configuration`, puis `VLAN Menu` et finalement `VLAN Support` , vérifier que le support est OK.
2. Définir les VLANs
   Ensuite, dans le menu VLAN, faire `VLAN Names` et ajouter les deux VLANs, le rouge et le vert. Par défaut, tous les ports du switch appartiennent au `DEFAULT_VLAN` qui a `1` pour numéro (`VLAN ID`). Il est important de **ne pas modifier ce VLAN par défaut**. Donner des VLAN ID différents pour les VLAN créés. Par exemple, **`20`** pour le VLAN **rouge** et **`30`** pour le VLAN **vert**.
3. Assigner les ports aux VLANs
   Dans le menu VLAN, faire `VLAN Port Assignment`. Chaque port est alors proposé pour chaque VLAN (défaut, rouge, vert), et *taggé* ou non : utiliser les VLAN rouge et vert

sans les tagger. Associer le rouge aux ports reliant le PC1 et le PC4 et le vert aux ports reliant le PC2 et le PC3.

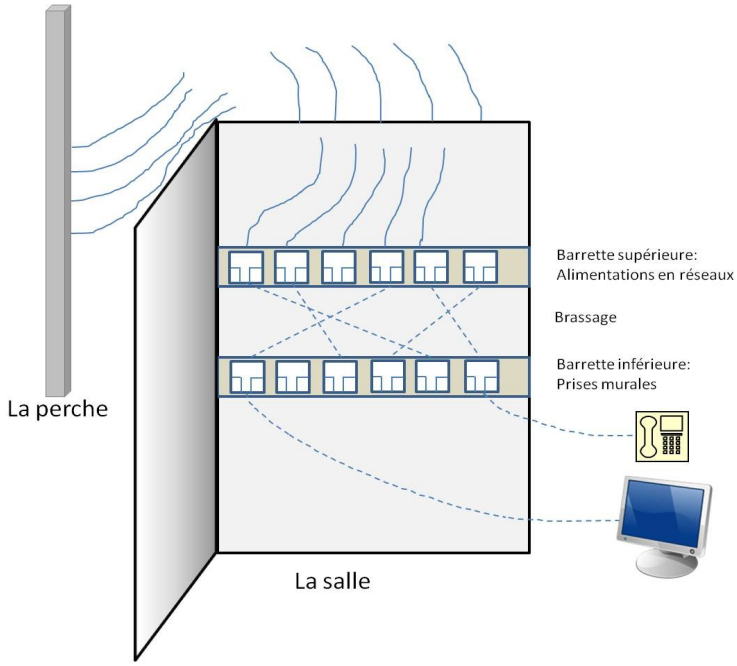
4. Tester alors la communication entre les différents PC et regarder l'activité du trafic sur les différentes interfaces, comme dans l'exercice 1. Expliquer ce qui se passe.
5. Vérifier en particulier si les broadcasts ARP générés par un ping d'une machine sur un VLAN atteignent ou non les machines de l'autre VLAN.
6. Donnez un accès internet au VLAN rouge. Que faudrait-il faire pour avoir un accès internet sur les deux VLANs ?

Remettez tout à son état initial

TP 2 - Câblage : fabrication de câbles et brassage

Description

Ce TP de câblage/brassage consiste principalement à fabriquer un câble et à installer une « mini-salle » avec une « mini-armoire de brassage ».
Le schéma de l'installation que vous avez devant vous est représenté sur la figure suivante. Les connexions (notamment en pointillés) ont uniquement un but d'illustration, et ne correspondent pas exactement aux numéros des prises que l'on vous demande d'analyser et trouver dans les questions du TP.



L'armoire de brassage que vous avez devant vous représente à la fois la salle pour laquelle vous allez devoir réaliser le câblage (donc les prises réseau aux murs de la salle), ainsi que l'armoire de brassage à laquelle ces prises murales vont converger et qui va vous permettre de donner aux utilisateurs de la salle l'accès aux réseaux que vous voulez, opération appelée *brassage*.

Dans l'état initial, 5 prises d'alimentation (i.e., venant de l'extérieur de la salle) sont câblées dans l'armoire de brassage et une prise est câblée vers les prises murales de la mini-salle.

- Dans une première étape, vous allez réaliser un câble Ethernet avec connecteurs RJ45, et en profiter pour vous remémorer sa structure et la fonction de chaque fil.
- Dans une deuxième étape, vous devez identifier les câbles entrant dans l'armoire et les connecter sur la perche selon les instructions.
- Ensuite, vous devez connecter les prises de « sortie » de l'armoire de brassage vers les prises murales selon les instructions données.
- Enfin, vous devez tester le câblage par le test de connectivité via le téléphone et l'ordinateur (ifconfig et ping).
- Finalement, visualisez les signaux Ethernet sur l'oscilloscope.

NB: les 2 PC à droite de l'armoire sont à votre disposition. Utilisez le noir pour l'accès Internet.

Questions

1. Fabriquer un câble RJ45 droit selon la norme TIA/EIA-568B:
- rappeler d'abord le code couleur et les fonctions des différents fils dans le rapport (voir fascicule annexe de TP et http://fr.wikipedia.org/wiki/RJ45)
- repérer comment numéroter les broches (*pins*) sur le connecteur RJ45
- Lisez entièrement la page : http://etienne.durup.free.fr/cablage/jecable2.htm, afin de comprendre comment est fait un câble, et ensuite en construire un.
- Une fois les étapes précédentes FAITES, appelez l'enseignant pour qu'il vous donne le matériel pour réaliser un câble droit (une extrêmité faite par chaque membre du binôme).
- Une fois réalisé, vérifier votre câble par le testeur de connectivité à votre disposition.
- Faites vérifier votre câble par l'enseignant.

2. Identifier les réseaux auxquels sont reliées les prises sur la perche. Les indiquer dans le rapport sous la forme « numéro de prise → adresse de réseau ».
- Détaillez le principe d'une prise double : comment peut-on avoir 2 réseaux sur le même connecteur RJ45 ?
- Pour la prise double, déterminez à quelles paires est attribué chaque réseau (en sachant que le premier réseau mentionné sur l'étiquette est attribué à la paire principale).

3. Déterminer quels câbles (identifiés par leurs numéros au stylo) d'alimentation de la mini-armoire doivent être liés à quelles prises de la perche si on désire pouvoir connecter les différentes prises murales (une seule prise murale est câblée pour l'exemple) aux:

  - soit réseaux 10.x soit réseaux 134.x (à l'aide de la prise double)

  - et réseau téléphonique

  et effectuez ces branchements.

4. Est-il possible d'avoir une prise double avec au moins un des 2 réseaux en Gigabit Ethernet ?

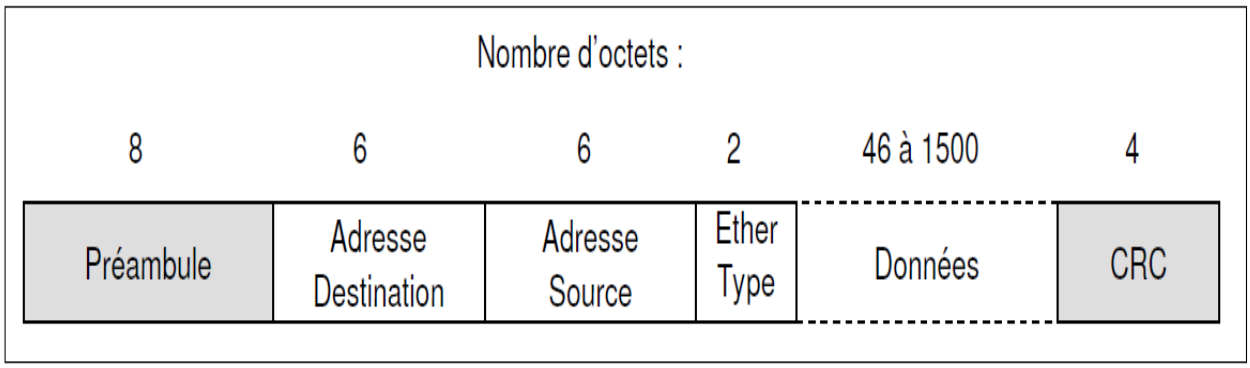
5. Sachant qu'au bout de la prise du réseau 10.x sur la perche se trouve un commutateur (cf. Configuration du réseau de la salle en page 3), devrait-on avoir un câble droit ou croisé pour la connexion allant du switch de la table où vous êtes à la prise murale reliée à la prise du réseau 10.x dans l'armoire ? Trouver une solution si l'on veut réaliser cette connecxion avec le câble qui ne convient pas a priori (mais ne pas toucher aux connexions du switch pour ne pas couper les autres binômes de la table du réseau).

6. Testez (uniquement écoute de la tonalité, ne le faites pas sonner, ça vous enlèverait des points) la connexion avec le téléphone, qui sera branché à une prise murale de la barrette inférieure de l'armoire.

7. Ensuite avec l'ordinateur, utilisez le script reseau10.sh pour changer la configuration réseau de votre machine, et tester ensuite votre connexion au réseau 10.x.

8. En envoyant un ping (qui aboutisse) vers le serveur de la salle 405, réalisez le branchement du câble gouttière sur l'oscilloscope. Visualisez les signaux Ethernet correspondants sur l'oscilloscope:
- quel signal visualise t-on (entrant ou sortant du PC) ?
- Faire un `sudo ping –f 10.4.105.253`, mesurez et justifier les signaux (forme, durée) en fonction des paquets envoyés. Vous devez obtenir l'allure des figures données dans le document (faire un capture à l'oscilloscope).

9. Analyse des résultats:
Nous rappelons que la trame Ethernet a le format suivant:

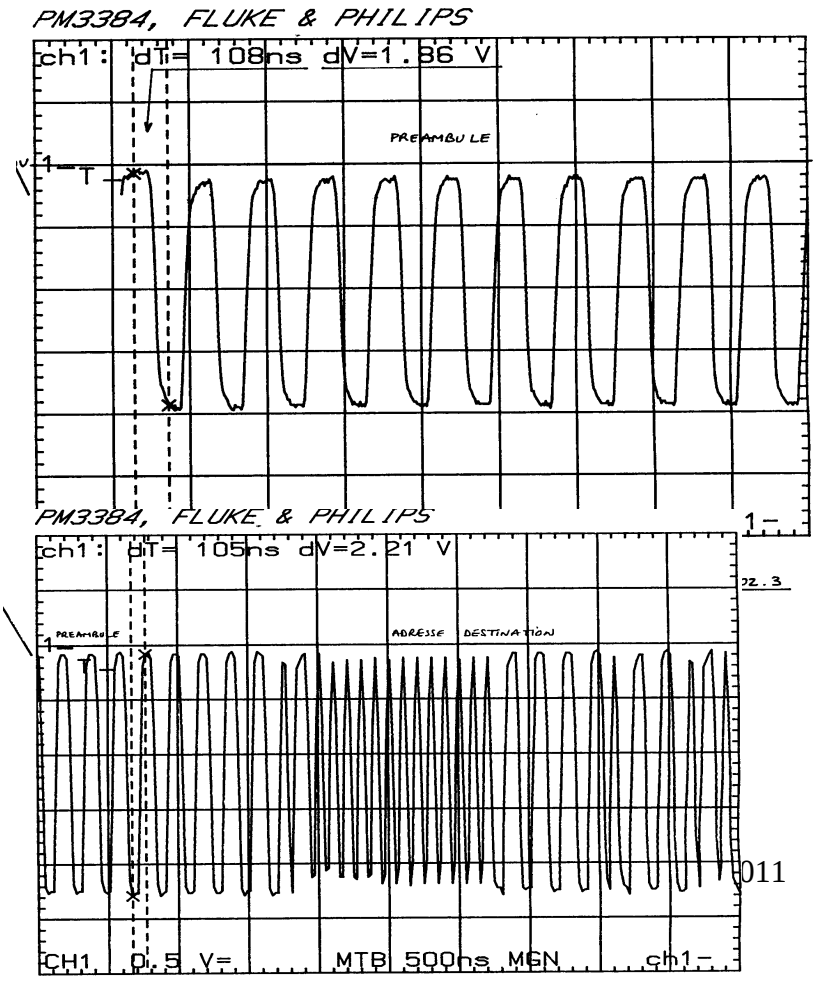


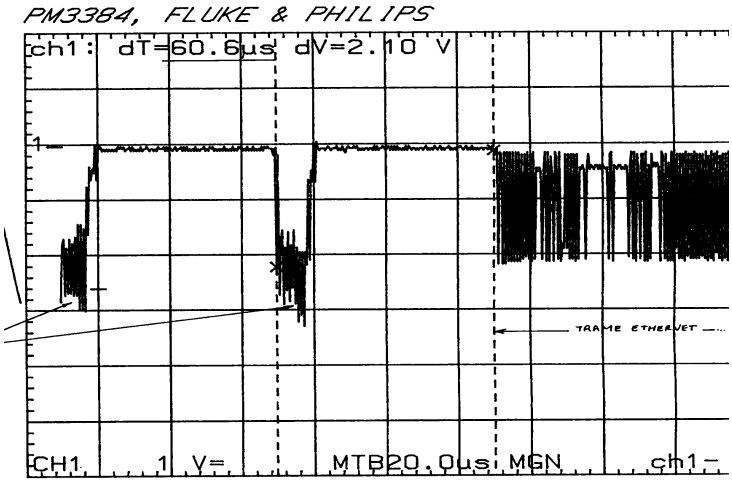
Format de la trame Ethernet V2

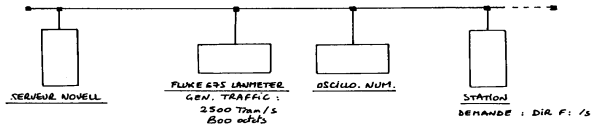
Le préambule est une suite de 0 et de 1 alternés. Il permet à l'horloge du récepteur de se synchroniser sur celle de l'émetteur.

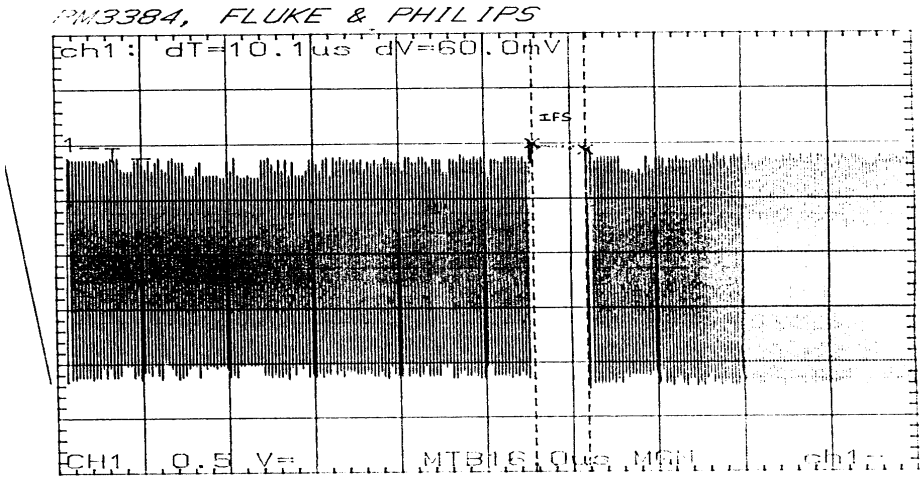
- Identifiez le préambule. A quoi le reconnaît-on ?
- Que dire de la durée du préambule par rapport à sa longueur ? Qu'en déduisez-vous sur le débit de la transmission ?
- Quelle est la durée totale de la trame Ethernet ?
- Est-ce cohérent avec la taille du message ICMP indiquée à l'écran ? Faites l'analyse en indiquant la longueur des différents *headers* rajoutés par les différentes couches protocolaires, et comparez.

10. Remettez tout en l'état initial









TRANSMISSION DE DEUX TRAMES ETHERNET
(avec Générateur de trafic FLUKE 675 LANMETER)

TP 3 - Simulation de réseaux avec OPNET

Introduction

Opnet est un logiciel de simulation de réseau. Contrairement à Wireshark ou à la sonde RMON, il ne permet non pas d'observer et analyser du trafic réel sur le réseau de la salle, mais de prévoir les performances d'un réseau « fictif » dont on lui fournit toutes les caractéristiques (topologie, équipements, types de trafic et charge).
(Le PC sur lequel vous travaillez est d'ailleurs déconnecté du réseau de la salle, utilisez le PC que vous avez à votre droite au cas où vous avez besoin de chercher des informations.)

Nous allons donc utiliser Opnet pour étudier et comprendre les performances d'un réseau local fonctionnant avec Ethernet dans différentes conditions, et notamment comprendre l'origine protocolaire des différences de performances si on utilise un switch ou un hub pour l'interconnexion.

NB : Vous devez suivre les étapes de configuration pas à pas rigoureusement. Le logiciel ne permet pas facilement de revenir en arrière dans la configuration du réseau.
En plus des explications détaillées, le rapport devra contenir des reproduction à la main de l'allure des courbes avec quantités et unités en abscisse et ordonnée.

Étude d'un petit réseau

Dans cette partie, on souhaite comparer les performances de deux réseaux simples comprenant chacun un serveur et trois clients, mais reliés par un hub ou par un switch. Pour chaque réseau, on va définir trois scénarios différents (on utilisera des liens 10BaseT) :

1. les 3 clients ont une faible activité ;
2. les 3 clients ont une activité très importante qui risque de surcharger le réseau ;
3. les machines ont une activité très importante, deux à deux.

Effectuez les étapes de configuration suivantes :

1. Lancez IT guru et créez un nouveau projet tp3_petit_votre_nom
2. Créez un scénario : tp3_hub, avec un environnement *Office*, d'une dimension de 100m x 100m et la technologie Ethernet.
3. Faîtes glisser trois stations Ethernet (ethernet_wkstn), un serveur et un hub dans la fenêtre de construction du réseau. Connectez les éléments au hub via des liens Ethernet 10 Mbps.
4. Ouvrez le projet TP_profile, copier les noeud Application et Profile, collez les dans votre projet.
5. Appliquez le profile *web* aux stations (sélectionner toutes les stations, ouvrez la fenêtre d'attributs (click droit), appliquez le trafic voulu dans la ligne *Application Supported Profiles.* Puis edit → ajoutez une ligne (Rows), n'oubliez pas de cochez *Apply changes to selected objects*.
6. Configurez le serveur en serveur « toutes applications » (ouvrez les attributs, ouvrez les applications, dans la fenêtre *Application Supported Services -> All*
7. Pour choisir le type de statistiques à observer, sous le menu *Simulation → Choose individual statistics*. Puis *Node statistics.* Pour cet exercice, on choisira les performances au niveau d'Ethernet : sélectionnez Ethernet.

8. Lancez la simulation, pour une durée de 30 minutes (*Simulation → Discrete event simulation*).
   Attention : il s'agit de simuler du trafic sur 30 min, mais simuler ce trafic et faire le calcul des performances ne prend que quelques secondes ! (le bip indique la fin de la simulation).

9. Dupliquez le scenario (*Scenario → Duplicate*), appelez le tp3_switch. Remplacez le hub par un switch (prendre le *ethernet16_switch*). Lancez la simulation pour une durée de 30 minutes.

Analyse des réultats :

10. Un fois les simulations terminées, allez dans *Results → View results* . Sélectionner un noeud correspondant à une station. Visualisez le délai au niveau Ethernet. Au niveau de la figure, sélectionnez *Overlaid statistics*, *average* et *All scenarios.* Cliquez enfin sur *Show.* Vous avez un figure que vous pouvez à présent analyser.
11. A quoi correspond le « délai au niveau Ethernet » exactement ?
12. Rappelez le fonctionnement d'un hub précisément : qu'advient-il d'une trame entrante ?
13. Rappeler le fonctionnement d'un switch précisément : qu'advient-il d'une trame entrante ? Décrire l'ensemble du processus de traitement au niveau du switch. (Rappelez-vous des tables d'adressage...)
14. Déduisez-en la raison pour laquelle vous observez ces performances en terme de délai.

Configuration :

15. Dans les deux scénarios, utilisez le profil d'application *haut débit* sur les stations, en veillant à ce que le champ *Application Supported Services* du serveur est toujours mis à *All services*. Dans les deux scénarios, appliquez un facteur multiplicatif de trafic de 10 (*Simulation → Configure Descrete Event Simulation →* Onglet *Global Attributes*, mettre l'attribut *Traffic Scaling Factor* à 10 et l'attribut *Traffic Scaling Mode* à *All Traffic*. Simulez sur trois minutes.

Analyse des réultats :

16. Comparez les performances et expliquez les différences (même manips qu'en question 10) :
    - Quel est le plus rapide (en terme de délai) dans ce contexte (hub ou switch) ?
    - Qu'est-ce qui a changé dans la configuration du réseau simulé pour obtenir ce changement ?
    - Expliquez le mécanisme CSMA/CD : définir l'acronyme et expliquez en détail à quoi ça sert et comment ça marche.
    - Visualiser les collisions (depuis le scénario hub). Que constatez-vous ?
    - En raisonnant sur le buffer de la couche liaison de données (sous-couche MAC) et sur les débits appliqués, expliquez l'allure de la courbe de délai (toujours au niveau d'une station) du switch et du hub (croissance au cours du temps pour le hub) ?

Configuration :

17. Ouvrez le projet TP_Trafic_spécifique. Dans ce projet, les lignes bleues représentent un trafic de 10 Mbps entre les paires d'équipements. Faites les simulations sur 3 minutes pour chacun des scenarios switch et hub.

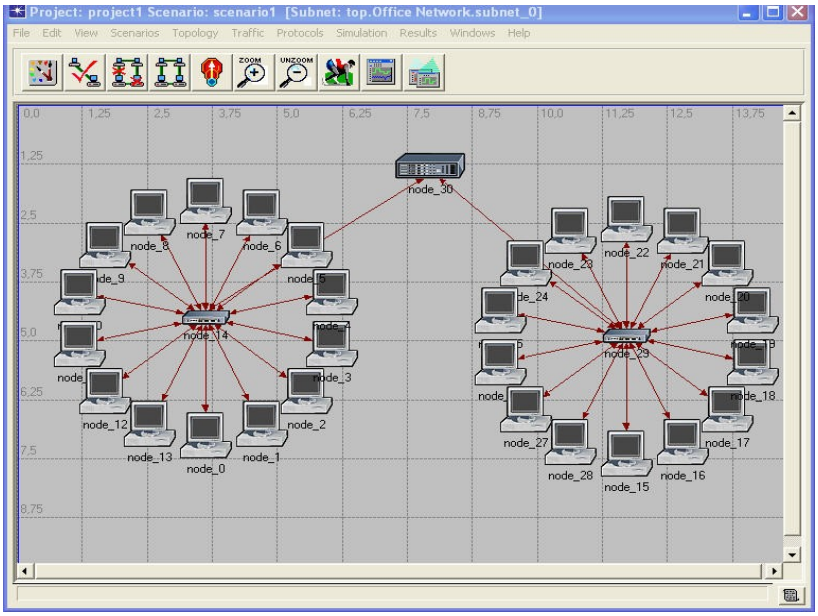
Analyse des réultats :

18. Affichez 4 fenêtres avec les charges de trafic -*load* en bits/s (correspondant au trafic émis) pour chacun des 4 noeuds. Dans chaque fenêtre doit évidemment apparaître 2 courbes, celle dans le cas du switch et celle dans le cas du hub.
19. Sachant que les câbles sont des 10BaseT, et que les cartes réseau permettent du 10Mb/s, que pouvez-vous dire sur la répartition du débit total par un hub et par un switch (raisonnez sur les valeurs précises et indiquez votre calcul) ?

Un réseau local plus important

Dans cette partie, on s'intéresse à un réseau local de plus grande taille. On souhaite dessiner l'architecture de ce réseau pour optimiser ses performances.

1. Créez un nouveau projet appelé tp3_grandlan_<votrenom>, créez un scénario vide appelé « hub », avec les même caractéristiques que précédemment.
2. Vous allez créer un sous-réseau. De la palette, faites glisser l'icône *subnet* dans l'espace de travail.
3. Double-cliquez sur le sous-réseau, ce qui va ouvrir une nouvelle fenêtre, la fenêtre du sous-réseau.
4. Créez une nouvelle topologie en utilisant le *rapid network configuration* : menu *topology → rapid configuration*. Choisissez la topologie *star*, *Ethernet hub* pour le centre et *Ethernet workstation* pour la périphérie (sélectionnez en 14). Utilisez des liens 100 BaseT.
5. Cliquez OK et IT Guru va générer automatiquement 14 workstations liées en topologie étoile à un hub.
6. Faites glisser le réseau, de manière à laisser de la place pour un autre réseau similaire.
7. Créez un deuxième réseau avec les mêmes caractéristiques.
8. Faites glissez un switch et connectez les deux réseaux au bridge. Donnez le nom de « bridge » au bridge (pour faciliter les étapes suivantes)

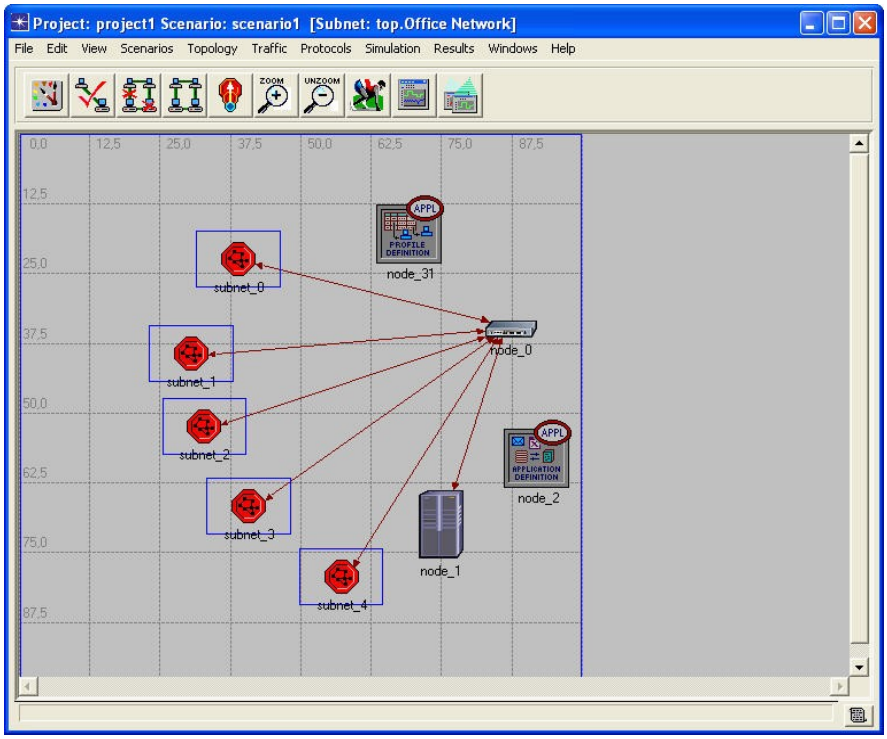


9. Retournez au sous-réseau racine en cliquant sur le bouton *Go to Parent Subnet* (5ème bouton)
10. Ouvrez le fichier TP_profile et recopiez les noeuds Application et profile.
11. Retournez dans le sous-réseau, sélectionnez toutes les stations (Ctrl-A), éditez les attributs (click droit) et choisissez le *application supported profile* web (*Edit → insert row ...*), N'oubliez pas de sélectionner le *Apply to selected Objects*.

12. Retournez au sous-réseau racine. Copiez le sous-réseau créé, et copiez le 4 fois - soit un total de 112 machines.
13. Faites glissez un hub et connectez le aux sous-réseaux avec des liens 100 BaseT. Vérifiez que vous connectez aux bridges des sous-réseaux.
14. Reliez le hub à un serveur Ethernet, configurez le en serveur pour toutes les applications (éditez les attributs, ...)
15. Appliquez un facteur multiplicatif de trafic de 10, Simulez sur 3 minutes.
16. Dupliquez le scénario, remplacez le hub par un switch, appliquez un facteur multiplicatif de trafic de 10, simulez sur 3 minutes.

Analyse :

17. Analyser les variables qui vous semblent d'intérêt comme par exemple le temps de réponse d'une page web, le débit et le délai au niveau TCP, ainsi que les paramètres déjà étudiés au niveau Ethernet.
18. Faites également varier la charge de trafic en transformant le profil « web » en « haut débit » comme dans la partie précédente. Notez vos observations.



TP 4 - Wireshark : analyse de trames Ethernet, ICMP et ARP

Introduction

Wireshark est un logiciel d'analyse de trafic. Il permet de contrôler la carte réseau de la machine sur laquelle il tourne, récupère les trames vu par la carte réseau et permet une analyse aisée des paquets. Le but de ce TP est d'abord de comprendre précisément la structure et la hiérarchie sous laquelle Wireshark présente les informations de trafic, en identifiant le rapport avec la normalisation du fonctionnement d'un réseau (notamment les différentes couches OSI). Une étude d'ICMP et d'Ethernet sera ensuite réalisée.

Ce logiciel est gratuit et existe sous Linux et Windows. N'hésitez pas à l'installer sur vos machines personnelles et à regarder ce qui se passe sur votre réseau en dehors des cours.

Ce TP se fait grâce à wireshark, qui est installé sur les machines virtuelles Linux. Lancer la machine virtuelle nommée « Pour_TP_R4 », se connecter en *user/user*, puis ouvrir un terminal et passer en root en tapant: *su*, password: *root*. Tapez *wireshark &* pour lancer le logiciel.
Comme pour les autres TP, toutes les étapes sont à faire dans l'ordre.

Prise en main

- Dans l'onglet Capture, cliquez sur Options. Sélectionnez l'interface sur laquelle la capture doit être réalisée (eth0 en général), décochez « *promiscious mode* » et les différentes « *name resolutions* ». Cliquez sur Ok. La capture est lancée.
- Connectez vous sur http://kheops.unice.fr. Une fois cette page chargée, arrêtez la capture.

Nous allons à présent procéder à une analyse structurée, « du plus général au plus détaillé », de la façon dont Wireshark représente le trafic.

1. Vous voyez que la fenêtre principale de Wireshark, où apparaît le résultat de la capture, est divisée en 3 sous-fenêtres. Cliquez sur une ligne. Donner la signification d'une ligne dans la première sous-fenêtre (celle du haut). Attention: on veut que vous identifiez l'entité générale représentée par une telle ligne, et non les détails de cette ligne.

2. Structure générale de la 2ème sous-fenêtre: que représente chaque ligne de cette sous fenêtre ? Attention, on ne veut pas des noms de protocoles spécifiques, mais que vous explicitiez la relation entre la 2ème sous-fenêtre et les couches OSI. Votre réponse doit être valable quelque soit le paquet sur lequel vous cliquez. Détaillez votre réponse.

3. 3ème sous-fenêtre : à quel alphabet appartiennent les symboles affichés dans cette fenêtre ? Que représentent-ils ? Cliquez sur une ligne de la 2ème sous-fenêtre. Que se passe t-il dans la 3ème ? A quoi cela correspond t-il ?

4. Identifiez à quoi correspondent exactement les parties surlignées pour chaque ligne de la 2ème sous-fenêtre dans la 3ème sous-fenêtre.

5. Quel processus général relatif au fonctionnement du réseau la 3ème sous-fenêtre vous permet-elle de voir ?

6. A quoi correspond le protocole indiqué dans l'avant-dernière colonne de la 1ère sous-fenêtre

?

Maintenant que la structure générale de représentation du trafic est identifiée, et que vous avez pu faire le lien direct avec votre cours réseau,. affichez le premier paquet « HTTP GET ».

6. Listez les protocoles utilisés sur le réseau. Pour chacun de ceux que vous connaissez, précisez dans quel(s) protocole(s) ils sont encapsulés.

7. Décrivez le processus d'ouverture d'une page web: but des différents paquets et protocoles aux différentes couches. (Rappelez vous vos TP de R1!)

8. Donnez le temps entre le « HTTP GET » et le premier « HTTP OK »

9. Donnez l'adresse IP de kheops.unice.fr et de votre machine. Comment s'assurer que les paquets que vous analysez sont bien les vôtres, et non ceux du binôme voisin qui fait le même TP ?

ICMP

Utilisez vos notes de cours sur ICMP, en particulier, les types de paquets ainsi que la signification du TTL (ou n'hésitez pas à aller chercher ces informations sur le web).

9. Enregistrez un ping vers kheops.unice.fr. Sélectionnez le premier « ICMP Echo Request », étendez les informations sur la partie de protocole IP : retrouvez votre adresse IP.

10. Combien d'octets contient l'en-tête IP ? Combien d'octets contient la charge de datagramme IP (encore appelée payload, pour « partie utile ») et comment déterminez-vous ce nombre ?

11. Le datagramme IP a-t-il été fragmenté ? Comment le déterminez-vous ?

12. Utilisez la commande `man traceroute` dans la console pour connaître le détail de traceroute. A quoi sert traceroute, et comment s'utilise t-il ? Que doit exactement renvoyer traceroute ?

13. Enregistrez maintenant un traceroute vers kheops.unice.fr : que voyez-vous exactement ? Est-ce le résultat attendu, pouvez-vous dire que ce traceroute a réussi ? Nous allons dans ce qui suit identifier la raison de cela.

Pour contourner le problème, dans la suite, vous utiliserez l'enregistrement wireshark d'un traceroute fait à partir d'une machine située l'extérieur du réseau local. Ouvrez le fichier traceroute.cap dans wireshark. S'il ne se trouve pas déjà sur votre machine, récupérez-le sur ftp://lserver.tp405/traceroute.cap, avec le login etudiant/Etudiant007, ou par « *scp etudiant@lserver.tp405:traceroute.cap .* » dans la console,

14. Quelle est l'adresse IP de la machine qui a été utilisée ?

15. Quel est le nom et l'adresse IP du serveur ciblé par traceroute ?

16. Quel protocole est utilisé par la machine cliente dans le cadre de traceroute ? Quel est le protocole utilisé pour la réponse à cette machine ?

17. Dans les résultats obtenus, quels champs des datagrammes IP changent TOUJOURS d'un message à l'autre ? Quels champs doivent rester constant, quels champs doivent changer ?

18. Trouvez la série de messages ICMP indiquant un TTL trop grand (TTL exceeded) envoyés par le routeur le plus proche. Quelles sont les valeurs du champ d'identification et du champ TTL ?

19. Faire la liste de tous les routeurs traversés.

20. Décrivez précisément le fonctionnement de traceroute.

21. Quel était donc le problème en question 13 ? (Pensez à la configuration du réseau local...)

Fragmentation

20. Utilisez la commande ping (voir `man ping`) avec une taille de paquet de 1472, puis 1473 puis 3000; faites ces 3 captures successivement, et après chacune, analysez les données ci-dessous pour répondre aux questions suivantes.

21. Observez les champs *IP id*, et les différents *flags* (à dérouler): à quoi correspondent-ils ? Quelle est la valeur du segment offset et pourquoi ?

22. Analysez le détails de IP et ICMP, pour comprendre la différence entre ce qu'il se passe pour 1472 et 1473. Notamment à quoi correspond 1518 ? (Pensez headers: allez chercher toutes les tailles d'entêtes pour pouvoir répondre).

Ethernet - ARP

Utilisez vos notes de cours sur ARP (ou informations appropriées sur le web). Faites un accès web sur www.mit.edu et capturez les paquets correspondants. On s'intéresse uniquement à la partie Ethernet.

22. Quelle est l'adresse Ethernet de votre machine ?

23. Quelle est l'adresse de destination indiquée dans la trame Ethernet ?

24. Est-ce l'adresse Ethernet du serveur www.mit.edu ? Pourquoi ? A quelle machine correspond cette adresse ?

25. Dans le message de réponse HTTP, quelle est la valeur de l'adresse Ethernet source ? À quelle machine correspond cette adresse ?

26. En utilisant la commande `arp -a`, affichez le contenu de la table arp.
27. Qu'est-ce qu'une table ARP ?
28. Videz la table arp (`arp -d @IP`).

29. Allez sur le site www.unice.fr, capturez les échanges et décrivez les échanges ARP en détail et leur but.

TP 5 - Wireshark : analyse de DHCP, FTP, SSH, mail

Vous pouvez relire la partie introductive du TP 4 pour lancer wireshark. Tout se fait sur les machines virtuelles Pour_TPR4.

Étude de DHCP

L'objectif de cette partie est d'observer précisément le mécanisme de configuration réseau automatique, ou DHCP. Reprenez votre cours sur DHCP et ouvrez la page suivante : http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol
Sur un des 2 PC du binôme l'interface va être désactivée et ré-activée, et l'autre PC va observer le trafic, ce qui est rendu possible car vos 2 PC sont connectés à un hub au bout de la paillasse.

- Lancez une capture wireshark en mode promiscuous (cf. TP4) sur PC1 et sur PC2 arrêtez et de redémarrez les fonctions réseau (`ifdown eth0` puis `ifup eth0`).

Examinez la capture pour décrire en détails le protocole DHCP :

1. Que signifie l'acronyme DHCP ?
2. Quel est le but exact du processus DHCP ?
3. Citez les 4 étapes du processus de configuration dynamique DHCP avec une description rapide de chacune d'elles.
4. Dans la capture identifiez et isolez chacun les paquets correspondant à chaque étape (attention de regarder les paquets correspondant bien à PC2, vous pouvez voir d'autres configurations d'autres PC de la salle qui démarrent, mais ne vous intéressent pas).
5. Pour chacun des ces paquets, rentrez dans le détail du protocole DHCP (Bootp), et observez que vous avec bien des formats de paquets et informations de la même forme que sur la page de wikipédia ci-dessus.
6. Pour chaque étape, donnez tous les **paramètres qui sont demandés** par le client au serveur, et donnez les valeurs que renvoie le serveur pour ces paramètres, spécifiques au réseau de la salle 405.

Étude de FTP

1. Donnez la signification de l'acronyme FTP.
2. Lancer une capture. Lancer une session ftp sur lserver.tp405 (`ftp lserver.tp405`), sous le login *etudiant* et password *Etudiant007*. Faites un `ls`. Puis `quit`. Arrêtez la capture.
3. Analyse de la capture : regarder les paquets FTP successifs et analyser leur contenu (donc au niveau application. Que dire du mot de passe ?
4. Que voyez vous dans la 2ème sous-fenêtre pour le détail de FTP ?
5. Quel est le rôle de TCP dans cet échange ?
6. Faites une analyse détaillée des ports TCP impliqués dans ces échanges, en rapport avec les commandes appelées.
7. Enfin, utiliser l'option *Follow TCP stream* sur les connexions d'intérêt.

Étude de SSH

1. Lancer une session ssh sur lserver.tp405: ssh etudiant@lserver.tp405.
2. Qu'observez-vous dans la trace ? Quel port TCP est à remarquer ?

Étude du protocole mail

1. Utilisez Kmail comme client mail (`kmail &` dans une console) :
   1. Configurez un nouveau compte avec le nom d'utilisateur etudiant, adresse etudiant@lserver.tp405, serveur entrant (POP3) lserver.tp405 serveur sortant (SMTP) lserver.tp405.
      POP: encryption : TLS for secure dl, Authentication methode : Plain
      SMTP : encryption : TLS, no authentication
   2. Effectuez une capture (wireshark) d'envoi et de réception d'emails. Analyser le protocole utilisé. Peut-on retrouver le mot de passe en analysant les paquets reçus ? Observez attentivement le protocole SMTP.
   3. Quels sont les ports TCP spécifiques à SMTP et POP ?

2. On va à présent utiliser une connexion telnet au serveur email pour envoyer et recevoir :
   1. telnet lserver.tp405 25 → d'où vient ce numéro ?
   2. helo lserver.tp405
   3. mail from: etudiant@lserver.tp405
   4. rcpt to: etudiant@lserver.tp405
   5. data
   6. blabla
   7. .
   8. quit
   9. Et pour recevoir :
   10. telnet lserver.tp405 110 → d'où vient ce numéro ?
   11. user etudiant
   12. pass Etudiant007
   13. list
   14. retr [numero de message]
   15. quit
   16. Observez la capture: qu'est-ce qui change par rapport à l'utilisation d'un client comme Kmail, à l'émission et à la réception ?

Utilisation des outils du menu *Statistics* pour l'analyse de trafic

1. Effacez la table ARP, lancez une capture et lancez une session http (web). Après capture, donnez le détail de tous les protocoles utilisés au cours de l'échange via l'outil *flow graphs*.

2. Faites une capture sur 2 minutes, en générant le plus de trafic différencié possible (download d'ubuntu par exemple).

3. Utilisez l'outil *IO Graphs* avec différents filtrages et indiquez les trafics captés.

4. Sur la même capture, utilisez les outils *Conversation*, *Endpoints*, et *Protocol hierarchy*.

5. En fonction des résultats, faites un bilan complet avec, d'une part, l'analyse du trafic, et d'autre part, les indications sur les protocoles utilisés et leurs interactions.

TP 6 – Sonde, logiciel Meterware : partie « RMON »

Dans les TP1, 4 et 5 notamment, le logiciel Wireshark est utilisé pour contrôler la carte réseau de la machine, et récupérer le trafic vu par cette carte, donc passant sur le câble relié au PC en question. Le logiciel permet ensuite une analyse du trafic.

La sonde RMON (modèle EtherMeter 1000e de Technically Ellite, placée en face de vous) en revanche est un matériel à part entière, qui peut elle-même analyser le trafic vu par sa carte réseau, et qui va ensuite renvoyer les informations sur ce trafic spécifiquement demandées par le logiciel interrogateur tournant sur un autre PC, en l'occurrence le vôtre. Le logiciel Meterware est le logiciel permettant le dialogue avec la sonde RMON.

RMON est un standard signifiant Remote MONitoring. Une sonde RMON est donc un agent qui va pouvoir être interrogé par une sorte de client, et ce grâce au protocole SNMP (Simple Network Management Protocol). Ce client récoltant les informations est appelé le manager SNMP. Vous verrez en fin de TP que ce dialogue SNMP est basé sur une certaine MIB, ou Management Information Base, normalisée, qui correspond à une structure en arbre aux différents niveaux duquel se trouvent des variables, dont la valeur peut nous intéresser et que l'on récupère donc.

Avant de commencer, lisez attentivement les pages 10 et 11 de la partie annexe en fin de fascicule. Toutes les réponses doivent être données par écrit.

Pour toutes les manipulations de ce TP, cette annexe vous sera très utile. Vous avez également à votre disposition le manuel d'utilisation de METERWARE.

Cartographie

Dans cette partie du TP, vous utiliserez la partie *Network map* pour dessiner un plan de la salle TP405, en se basant sur la description du réseau de la salle en début dufascicule de TP. Y figurera :
- le hub de la paillasse opposée sur lequel sont branchés les 2 PC à votre disposition
- la sonde à IP fixe liée à ce hub
- le switch de la salle de brassage qui est relié à ce hub par la perche
- le serveur et la passerelle (pas reliés directement au hub)

Cette cartographie vous permettra notamment de visualiser quelles machines sont actives, mais également quelles adresses sont actives dans l'espace DHCP de la salle.

1. Après avoir pris note de toutes les machines présentes, faites un tableau PAR ECRIT de toutes les machines et de leurs adresses MAC et IP.

2. Pourquoi connecte t-on la sonde à un hub, et non un switch ?

3. Pour ajouter des équipements dans *Network map*, faire *Edit → New device*
4. Ajouter d'abord la sonde, puis les autres équipements. La sonde étant un équipement supportant SNMP, vous pouvez ne rentrer que le nom et l'@IP, appuyez sur *resolve* et les informations sont récupérées. Changez les communautés de lecture et écriture à *hp_admin*.

5. Une fois toute la topologie créée, utilisez la fonction Quick View de la sonde pour avoir une idée rapide de ce qui se passe dans la salle.

6. Comment la sonde estime t-elle l'état (la valeur) d'une variable que Meterware récupère ? Faites varier le *Sampling interval* (à trouver dans le menu) pour inférer la réponse.

7. A quoi correspond le premier graphique Packets/s : de quels types de paquets s'agit-il exactement (quelle couche OSI) ? Que représentent les ordonnées ? Que représente le nombre 1518 ?

8. Comment est calculée l'*utilisation* affichée en pourcentages (quelles sont les quantités concrètes qui interviennent dans ce calcul – débits impliqués) ?

Le groupe « statistics » de la sonde RMON (groupe RMON)

Consultez les pages afférentes au groupe Statistics dans le manuel de Meterware.

5. Dans un premier temps, réinitialisez les données de la sonde. Indiquez comment vous faites. Quelle influence sur les mesures ?

6. Parcourez chaque fonction (dans l'onglet *View*) du menu Statistics.
7. Vous pouvez utiliser votre PC et/ou le PC de gauche pour générer du trafic de façon à, par exemple, voir des erreurs.

8. Détaillez ce que permet de représenter chaque fonction (et chaque sous graphique donc). On ne vous demande pas de recopier, mais de montrer que vous avez saisi la signification des graphiques. Indiquez notamment comment sont calculées les quantités représentées.

9. Notamment, quel est la différence entre mesure instantanée et mesure cumulative ?

10. Que déduisez-vous du type de trafic circulant sur la portion de réseau visible par la sonde ?

Groupe « TOPN »

Utilisez le groupe « TOPN » :

1. Quels types de paquets (quels couches OSI) sont représentés exactement sur le « camembert » ? Que dire de la légende ?
2. Identifiez les équipement les plus bavards. Justifiez vos résultats en fonction des adresses des équipements (serveur, passerelle, etc.)
3. Utilisez la machine libre pour générer du trafic intense (`ping -f 10.4.105.253` ou download d'ubuntu...) et vérifier les résultats de TOPN.

Groupe « MATRIX »

Utilisez le groupe « MATRIX »:

1. Qu'est-ce qui est représenté ?
2. Quelle différence entre *View Cumulative* et *View Delta* ?
3. Identifiez les paires d'équipements qui ont le plus d'échanges.
4. Vérifiez par rapport au trafic que vous avez généré au point précédent.
5. Utilisez le filtrage d'adresses pour identifier le trafic généré par le PC de gauche.

Groupe « ALARM/EVENT »

Dans un premier temps, utilisez le menu général (c'est-à-dire non lié à la sonde) pour générer une alarme indiquant un dépassement de charge du réseau de 10% :

1. Que veut-on dire par « charge du réseau » ? Donner un définition en terme de quantités concrètes.

2. Créez cette alarme.

3. Regardez les détails (sélection puis *modify*) de l'alarme apparaissant dans le menu ALARM de la sonde :
   1. A quoi correspond la case *Variable* ?
   2. Grâce à votre réponse à la première question de cette partie, expliquez les valeurs des cases *Threshold – Rising* et *– Falling*. Donner notamment le **calcul exact** permettant de retrouver 1250000 en *Rising threshold*.

4. Générez un trafic important sur la machine libre (par exemple `ping -f kheops.unice.fr` ou download d'ubuntu) et vérifiez que l'alarme a bien été déclenchée (dans les logs). Si l'alarme ne se déclenche pas, pensez à regarder votre débit de téléchargement par exemple, et à baisser le seuil de l'alarme le cas échéant pour voir le déclenchement.

5. A l'aide du point précédent et du manuel, créez les alarmes suivantes, directement à partir du menu de la sonde :
   1. charge supérieure à 20% de la bande passante
   2. charge inférieure à 30% de la bande passante
   3. nombre de paquets de taille supérieure à 1024 supérieur à 100 par seconde
   4. nombre de collisions compris entre 10 et 100 par seconde

   Pour chaque point, indiquez dans le rapport les valeurs exactes mises dans chaque case de configuration de l'alarme. Vérifiez en générant un trafic adéquat.

Groupe « Capture / Filter »

Utilisez le groupe « Capture / Filter » pour :

1. Filtrez (= ne laissez passer que) les requêtes ARP: créez un filtre (et enregistrez-le), un canal, puis attachez le filtre au canal. Lancez la capture en faisant en sorte de générer les paquets voulus, et analysez le buffer.
2. Filtrez les paquets émis vers votre machine de la même façon.
3. Analyser les paquets. Donnez le détail des informations fournies par Meterware et comparez avec ce que wireshark vous donne.
4. Quelle différence dans la méthode de capture par rapport à wireshark ?
5. Déclencher une capture / un filtrage grâce à une alarme générée

Tout remettre dans son état initial

Effacer tous les équipements, liens et alarmes.

TP 7 – Sonde, logiciel Meterware : partie « RMON2 »

Pour toutes les manipulations, outre les documents fournis, utilisez le manuel d'utilisation de METERWARE disponible en salle de TP. Se référer au TP 6 pour la création de la sonde. Ne pas oublier de changer les communautés de lecture et écritue de la sonde à *hp_admin*.

Démarrage

Dans la fenêtre de départ, créez la sonde et faites un Quick view dans un premier temps pour surveiller l'activité du réseau : rappelez à quoi correspondent les 3 graphiques.

Prot Admin

Utilisez le groupe Prot Admin :

1. Fenêtre en haut à gauche : expliquez pourquoi chaque protocole (notamment Ether2 et ceux qui lui sont liés) sont situés à ces niveaux spécifiques de l'arborescence (liens avec couches OSI) ? Quel processus d'accès au réseau structure donc cette arborescence ?
2. Pourquoi un même protocole peut se retrouver plusieurs fois à un même niveau de l'arbre ?
3. Quels protocoles sont reconnus au niveau RMON2 ?
4. Expliquer ainsi ce que représentent exactement les barres de l'histogramme de la fenêtre en bas à droite. Pourquoi un même protocole peut apparaître plusieurs fois dans l'histogramme ? Que signifient les lettres devant son nom ?

Prot Stats

1. Allez dans *Options → Select protocol* : dans quelle fenêtre se voit votre choix ?
2. Diagramme en haut à gauche : générer une requête ARP. Vous voyez deux parties différentes dans le diagramme. A quoi correspond ce diagramme ?
3. Cliquez sur chacune des ces parties successivement. Qu'observez vous sur le diagramme en haut à droite à chaque coup ? Que représente t-il ? Pourquoi ?
4. Enfin cliquez sur chacune des parties du diagramme de droite. Qu'observez-vous sur l'histogramme du bas ?
5. Quel équipement / quelle application est à l'origine de la plupart du trafic UDP / SNMP ?

Host NL / Host AL

1. Utilisez le manuel pour afficher un diagramme tel qu'à la page 116 du manuel.
2. Faites une cartographie (par écrit) des protocoles les plus utilisés en concordance avec les machines utilisées.
3. Limitez la liste des protocoles IP affichés à 30 entrées (vérifiez au niveau de la table de contrôle).
4. Afficher uniquement les paquets des machines de 10.4.105.1 à 10.4.105.63. Décrivez le calcul sur les masques réseau pour pouvoir faire cela.

Trafic externe

1. Demandez à l'enseignant de simuler un trafic externe. Utilisez les groupes « host NL », « matrix NL » et « Addr Map » pour analyser le trafic généré. Donnez une cartographie la plus complète possible du trafic généré.

2. Filtrer les paquets échangés entre votre machine et le serveur, alternativement dans le sens montant puis descendant.

MIB

Allez dans MIB Browser dans le menu général. Trouver « rmon » et indiquez, en utilisant les outils « MIB », la structure de base de données utilisée.

Tout remettre dans son état initial.

ANNEXES

Gestion de câblages réseau : principe de base et segmentation

Introduction

L'objectif de cette manipulation est de s'informer sur les principes de base d'un système de câblage d'une entreprise d'en évaluer les contraintes. Les entreprises doivent veiller à une adaptation de leur structure aux évolutions des marchés et des technologies qui se traduit par :
L'arrivée de poste de travail de plus en plus sophistiqué (téléphone, fax, informatique),

L'accroissement du nombre d'ordinateurs et l'augmentation du débit,

L'hétérogénéité des équipements,

La mobilité des personnes d'un bureau à un autre,

La mise en place de ressources communes (serveurs et imprimantes).

Il faut donc rendre "intelligent" le bâtiment accueillant l'entreprise en y installant un câblage normalisé, perfor-mant et suffisamment dimensionné pour répondre aux besoins évolutifs des entreprises. Le systéme de câblage des courants faibles (informatique et téléphone) représente un coût de l'ordre de 3 à 5% du coût total de construction d'un bâtiment. Il doit donc permettre le raccordement d'une gamme de matériels et de services suffisamment large pour répondre aux besoins pour au moins les dix années à venir. Du fait des progrès technologiques et de l'hétéro-généité des matériels, le câblage doit répondre à des normes. Les normes internationales (EN 50167 / 50168 / 50169 / 50173 / 50174 et ISO/CEI 11801) spécifient les règles assurant notamment les hauts débits et les compatibilités électromagnétiques (CEM). Enfin, les entreprises réclament des espaces de travail facilement transformables et reconfigurables en fonction de l'évolution de leur organisation. Pour satisfaire aux contraintes, il s'agit donc de concevoir un système de câblage prenant en compte les principes suivants :
Distinction des courants forts et courants faibles :

- un point d'accès doit disposer de deux prises "courant fort" dont une au moins secourue
- le dimensionnement en "courant faible" doit prévoir deux raccordements (téléphone / informatique)
- les chemins de câble "courant fort" et "courant faible" doivent être distincts pour les CEM

Performances adaptées aux services utilisés,

Optimisation des coûts d'installation puis d'exploitation,

Conformité aux normes internationales,

Souplesse d'exploitation, c'est-à-dire pas de réinterventino sur la partie fixe du câblage,

Pas de préaffectation de câbles et de points d'accès,

Raccordement de chaque point d'accès par quatre paires,

Banalisation des prises de raccordement au niveau des points d'accès.

Architecture générale d'un système de câblage interne en courant faible

Dans un système de câblage "courant faible", on distingue six parties bien distinctes :
Le répartiteur général

Les répartiteurs de distribution

Les câbles de distribution

Les câbles de rocade

Les câbles capillaires

Le *répartiteur général* est le point central de raccordement des câbles du réseau public, des câbles de raccordement du PABX et de diverses liaisons téléphoniques ou informatiques, des câbles de distribution et de rocade. Les *répartiteurs de distribution* sont les nœuds de concentration des câbles vers les points d'accès. Ils comportent les câbles de distribution, les câbles de rocade, les câbles capillaires et les équipements actifs de réseaux (hub, pont, switches, routeurs, passerelles, multiplexeurs, concentrateurs, répéteurs, transceivers). Les *câbles de distribution* relient le répartiteur général aux répartiteurs de distribution. Ils supportent principalement les liaisons directes au téléphone commuté RTC, les liaisons spécialisées et les liaisons derrière le PABX.

Les *câbles de rocade* relient les répartiteurs de distribution entre eux. Ils supportent principalement les liaisons informatiques et sont matérialisés par des **connecteurs verts**. Les *câbles capillaires* relient directement chaque répartiteur de distribution aux points d'accès et sont posés en étoile (les **connecteurs** sont **bleus**). Enfin, les *points d'accès* sont les prises murales destinées au raccordement des terminaux téléphoniques et informatiques. Chaque point d'accès correspond à un certain nombre de prises "courant faible", "courant fort non secourue" et "courant fort secourue".

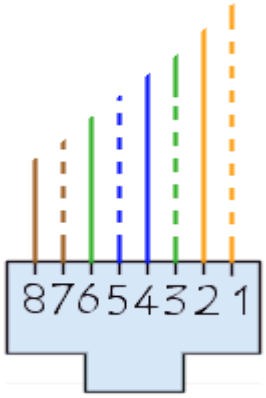
Philosophie du pré-câblage

Le pré-câblage est une notion de câblage par anticipation afin d'éviter les extensions au fur et à mesure de l'expression des besoins dues aux évolutions technologiques contribuant à une transformation rapide des réseaux. Le coût du câblage se composant de main d'œuvre et de fourniture, reste élevé alors que les équipements d'interconnexion et de transmission baissent régulièrement. D'autre part, le pré-câblage se justifie par la nécessité d'offrir aux entreprises, des espaces de travail adaptables, sans devoir tirer de nouveaux câbles, sans modification des locaux et sans gêner les occupants dans l'exercice de leur travail.
Pré-câbler une entreprise réside en la pose d'un réseau de conducteurs et de points de connexion en quantité, en qualité et en flexibilité d'arrangement suffisantes afin de pouvoir relier deux points quelconques du bâtiment par n'importe quel type de réseau. Il faut donc posséder des prises en tous points du bâtiment afin de permettre le raccordement des postes de travail ou leur déplacement sans avoir à repasser le câble. La reconfiguration topologique des réseaux en place est ainsi possible sans modification structurelle du câble. Le pré-câblage est donc un investissement profitable car il minimise les dépenses ultérieures.

Les normes et les aspects techniques

En France, l'AFNOR et l'UTE, membres respectivement de l'ISO et de la CEI, ainsi que des associations de professionnels comme France Télécom ont édité des spécifications. Ainsi, la norme ISO/CEI 11801 définit les paramètres à mesurer et les valeurs à respecter pour les connecteurs, permettant d'identifier des **catégories** (voir cours):

Les connecteurs RJ45 (wikipedia)



Connecteur RJ45 vu de face (fils vers l'arrière), norme TIA-568B

Un connecteur **RJ45** est une interface physique souvent utilisée pour terminer les cables de type paire torsadée. « RJ » vient de l'anglais *Registered Jack* (prise jack enregistrée) qui est une partie du Code des réglements fédéraux (*Code of Federal Regulations*) aux États-Unis. Il comporte 8 broches de connexions électriques.

Il est souvent utilisé avec des standards comme le TIA-568B qui décrit le brochage de terminaison du cablage (le standard TIA-568A est identique avec les couleurs orange et vert inversées).

Une utilisation très courante est le cablage ethernet qui utilise habituellement 4 broches (2 paires). D'autres applications sont par exemple les connecteurs des téléphones de bureaux ou les application de réseaux informatiques comme l'ISDN et les T1.

Câblage

Lors d'un cablâge informatique, seul les broches 1-2 et 3-6 sont utilisés pour transmettre les informations.

Câblage droit

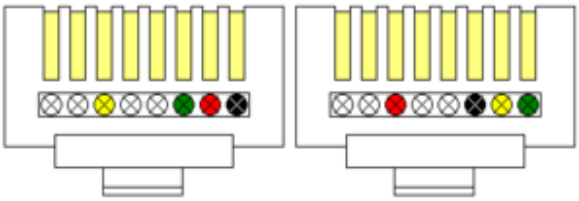
N° Broche	***N° Paire***	***Couleur***	---- ---- ----	***Couleur***	***N° Paire***	***N° Broche***
1	3	Blanc-orange		Blanc-orange	3	1
2	3	Orange		Orange	3	2
3	2	Blanc-vert		Blanc-vert	2	3
4	1	Bleu		Bleu	1	4
5	1	Blanc-bleu		Blanc-bleu	1	5
6	2	Vert		Vert	2	6
7	4	Blanc-brun		Blanc-brun	4	7

8	4	Brun		Brun	4	8

Cablâge croisé

N° Broche	*N° Paire*	*Couleur*	-------- -----	*Couleur*	*N° Paire*	*N° broche*
1	2	Blanc-vert		Blanc-orange	3	1
2	2	Vert		Orange	3	2
3	3	Blanc-orange		Blanc-vert	2	3
4	1	Bleu		Bleu	1	4
5	1	Blanc-bleu		Blanc-bleu	1	5
6	3	Orange		Vert	2	6
7	4	Blanc-brun		Blanc-brun	4	7
8	4	Brun		Brun	4	8

Fabriquer un RJ-45 avec un cable téléphonique

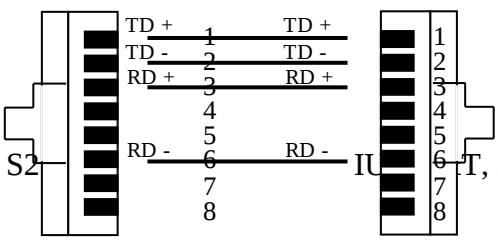


Le cablage à un bout du cable, et à l'autre bout. Seul ces 4 bornes transmettent réellement l'information, les 4 fils de cuivre téléphoniques (couleurs) sont suffisant.

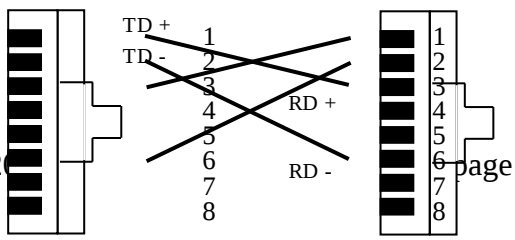
Les réseaux éthernet 100Mb en TCP-IP n'utilisent en fait que 4 fils des 8 fils des RJ-45. On peut donc fabriquer soi-même un câble réseau RJ-45 avec un câble 4 brins tel que les câbles téléphoniques (accordéons, ressorts, etc, qui eux ne contiennent que 4 fils). Le point important est que les prises de début et fin présentent chaque fil à la bonne place.

Ceci permet de fabriquer soi-même des cables réseaux avec des câbles téléphoniques, spiralés, qui sont plus pratique car moins encombrants, se contractant automatiquement par effet ressort, comme tout câble de téléphone.

Le connecteur RJ45 est utilisé avec des câbles UTP ayant une distance maximale de 90 mètres. Il existe deux manière de fabriquer un cordon de connexion RJ45/RJ45 selon les équipements à interconnecter. Un câble droit permettra de connecter une carte réseau à un équipement d'interconnexion (Hub, Switch). Une câble croisé est utilisé afin de relier deux équipements d'interconnexion, notamment entre deux hubs en cascade ou entre le switch et ses différents hubs segmentés. Voici la manière de fabriquer ces deux types de câbles :



Câblage droit RJ45/RJ45 : MDI



Câblage croisé RJ45/RJ45 : MDI-X

Mais attention, la fabrication des câbles varie selon les types d'équipements d'interconnexion connectés. Ainsi, pour connecter un hub avec certains MAU (Medium Attachment Unit) utilisés dans le câblage Token-Ring, il faudra croiser les broches par paires, soit croiser les fils 1 et 2 puis les fils 3 et 6.

Mise en œuvre : sonde Rmon2 et logiciel Meterware

Introduction

De plus en plus d'administrateurs de réseaux locaux sont soucieux d'une optimisation des transferts d'informations au sein de leur entreprise, notamment en ce qui concerne les flux des messageries électroniques, des accès aux serveurs WEB et des flux d'impression. Ces observations sont réalisables à partir d'une campagne de métrologie menée sur des interconnexions de réseaux locaux. A partir des informations issues de cette campagne, l'administrateur pourra repérer entre autres, les plus bavards, les équipements générateurs d'erreurs, les segments saturés et pourra réorganiser son réseau en conséquence. Les matériels nécessaires à cette campagne se composent d'une sonde Rmon2, 10Mbps (processeur Intel i960CF 25 MHz, 50 MIPS : la fiche technique figure en **Annexe1**) que l'on dispose sur les segments à observer, ainsi que du logiciel Meterware nécessaire pour piloter la sonde et utiliser ses données. L'objectif de cette manipulation est dans un premier temps, d'apprendre à installer et configurer la sonde Rmon et le logiciel Meterware, puis dans un second temps, de s'initier à certains services Rmon, afin de pouvoir mener ultérieurement des campagnes de métrologie.

Métrologie

La métrologie est la science des mesures. La métrologie des réseaux locaux consiste donc en la mesure de toutes les caractéristiques qui les définissent. Ces mesures portent notamment sur l'utilisation du média par les machines ainsi que sur les dysfonctionnements qu'elles peuvent présenter. Il faut écouter le support et étudier tout ce qui circule dessus. Pour cela sont utilisés des matériels d'audit de réseau tels que les sondes Rmon (Remote MONitoring) et leur logiciel de pilotage Meterware. Toutefois, il est nécessaire de connaître certaines notions théoriques telles que les équipements d'interconnexion afin de savoir où placer la sonde Rmon (répéteur, pont, routeur, switch, tranceiver), le protocole d'admistration SNMP, le réseau IUT du site de Sophia-Antipolis et la numérotation des adresses ou la notion de masque de sous-réseaux.

Le protocole d'administration SNMP : (Simple Network Management Protocol)

Les protocoles d'administration de réseaux permettent à un administrateur de superviser les éléments interconnectés. Les équipements interconnectés et les réseaux pouvant être hétérogènes, le logiciel d'administration est vu comme un programme d'application utilisant les couches Transport et en-dessous. **SNMP** n'est pas une norme mais un projet de norme contenu dans la famille des protocoles **TCP/IP**. C'est un standard dont la diffusion est telle qu'il peut être assimilé à une norme.

Quelques mots sur la couche Transport

Le protocole TCP est un protocole avec connexion. Il offre les facilités suivantes :
Contrôle de flux par une technique de fenêtrage,

Adressage de/vers un port,

Détection et récupération d'erreurs (checksum, temporisation et retransmission),

Contrôle du séquencement,

Indication d'urgence de données

Sélection des numéros initiaux de séquence

Demande de fermeture

Les applications couramment utilisées au-dessus de TCP sont FTP (File Transfer Protocol) et Telnet. Il existe le protocole **UDP** qui est un protocole sans connexion. Il est utilisé pour des besoins spécifiques en temps réel. Il présente l'avantage de livrer avec le meilleur effort en terme de délai, mais les inconvénients majeurs sont l'absence de récupération des paquets perdus ou détériorés, l'absence de contrôle de séquencement et l'absence de contrôle de flux. UDP est très utilisé notamment pour NFS (Network File System).

Les requêtes SNMP

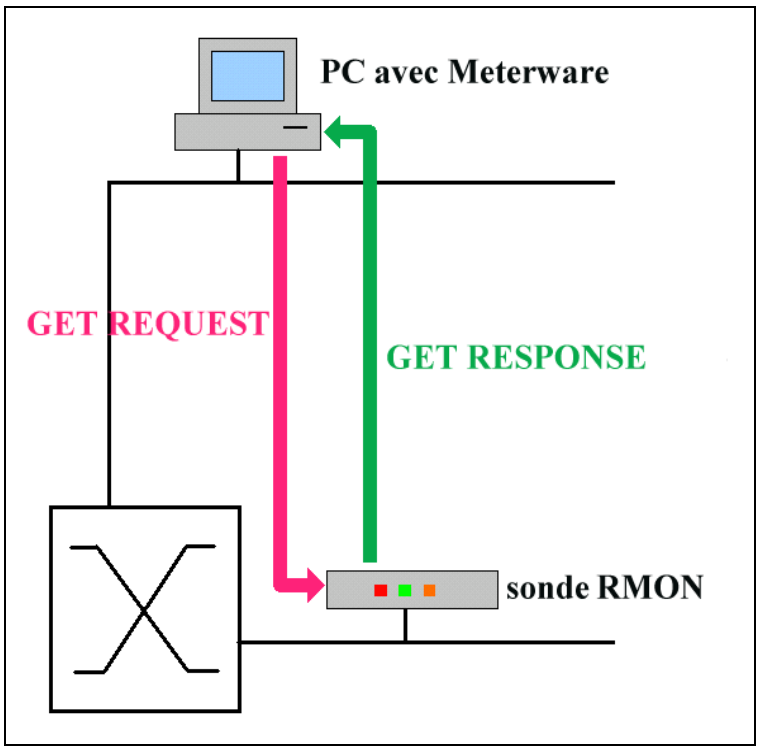
SNMP n'est conçu qu'autour de deux commandes : «aller chercher» et «enregistrer». Ceci permet une grande stabilité de ce protocole, même si de nouveaux éléments viennent enrichir la base de données. Au travers de ces deux commandes, on peut effectuer diverses opérations comme le reboot d'une machine, l'envoi d'un message sur un événement (trap), le rapatriement d'informations enregistrées par des équipements disposant d'agents SNMP, …
Un agent SNMP est un agent implémenté par la plupart des constructeurs d'équipements administrables permettant de conserver des données relatives à l'état des interfaces réseaux, aux trafics entrants et sortants, aux erreurs détectées sur les supports, aux signaux de contrôle interceptés.

Un message SNMP se compose de 3 parties essentielles :
Une version de protocole,

un identificateur de communauté SNMP,

une zone de données contenant 1 ou plusieurs PDU (Protocol Data Unit).

SNMP est donc un protocole qui permet à un administrateur d'accéder à ces informations. Ces informations sont structurées en base de données d'administration de réseau ou MIB (Management Information Base). La MIB standard définit les informations à gérer sur n'importe quel équipement administrable. Malheureusement la concurrence entre divers bâtisseurs de protocoles d'administration a débouché sur la création d'extensions spécifiques aux protocoles. Ainsi l'extension MIB-II est proposé sur SNMP. Les constructeurs d'équipements fournissent également leur « MIB constructeur » en complément à la MIB standard.
La sonde RMON est un équipement électronique disposant d'un agent SNMP, d'une mémoire program-mable et d'une mémoire volatile. Sa fonction essentielle est de stocker dans une MIB les statistiques relatives au segment LAN sur lequel elle est reliée. Les statistiques fournies par ce type de sonde seront étudiées dans les TP spécifiques de métrologie. La consultation de ces informations s'effectue donc au travers de requêtes SNMP formulées par une station d'administration. Les requêtes permettent d'une part de comptabiliser des événements particuliers et de stocker ces indications dans la mémoire volatile de la sonde et d'autre part de rapatrier ces informations sur la station. La station d'administration est un micro-ordinateur sur lequel est installé une carte réseau, un OS de type WindowsNT ou 95 et le logiciel de pilotage des sondes MeterWare. Le logiciel MeterWare offre une interface graphique simplifiant considérablement l'apprentissage et l'utilisation de l'outil de métrologie. En fait, ce logiciel élabore les requêtes SNMP à partir des services proposés et présente graphiquement, de manière plus conviviale, les données récupérées sur la sonde. Le schéma ci-dessous résume le dialogue entre une sonde Rmon et le logiciel MeterWare :



Il existe 4 niveaux d'accès à la sonde, permettant de garantir une hiérarchie limitant l'accès aux fonctions et aux données de la sonde. Les 4 niveaux sont donnés ci-dessous :
niveau1 : accès en lecture uniquement, pas d'accès aux fonctions RMON,

niveau2 : accès en lecture uniquement, accès aux services RMON mais pas d'accès au buffer des captures,

niveau3 : accès en lecture uniquement, accès aux fonctions RMON en lecture et en écriture,

niveau4 : accès en lecture et en écriture à toutes les MIBs de l'équipement.

Il est donc possible de limiter l'utilisation de la sonde selon l'utilisateur par le biais de ces niveaux. Pour cela, il faut créer des **communautés** auxquelles seront rattachées les adresses IP des machines de management. La procédure à suivre est la suivante :
Au moment de la configuration de la sonde, des communautés sont créés en leur attribuant un nom et un niveau d'accès à partir du menu «*Trusted Community Names Configuration*»,

Ensuite dans le menu «*Trusted Client IP Hosts Configuration*», l'adresse IP de la machine devant accéder à la sonde est définie, puis il faut attribuer un masque (permettant d'autoriser d'autres adresses IP à partir de la première et la communauté à laquelle il appartient).

La sonde est bien entendu configurée d'origine avec des communautés afin de permettre une utilisation immédiate. Cette configuration autorise toutes les machines par défaut. Afin d'autoriser l'accès aux fonctions et aux données, la sonde fonctionne de la manière suivante :

Le client désirant accéder à la sonde fournit son @IP et le nom de la communauté à laquelle il appartient (le nom de la communauté peut donc être assimilé à un mot de passe),

La sonde récupère cette adresse et effectue un «et logique» avec le masque,

Le résultat est comparé avec l'@IP configurée et si les deux adresses sont identiques, le client est autorisé.

Par exemple, pour que les machines ayant comme @IP 134.59.137.96 et 134.59.137.97 aient accès

à toutes les fonctions de la sonde, il faut récupérer dans la configuration de la sonde, le nom de la communauté de niveau 4. Ensuite doit être créé une entrée dans le menu «*Trusted Client IP Hosts Configuration*» :

Le nom de la communauté doit être défini,

En écrivant les deux @IP sous forme binaire, seul le dernier bit diffère. Il faut donc créer un masque rempli de 1 avec des 0 à l'emplacement des bits pouvant varier. Le masque appliqué aux deux machines est égal à 11111111.11111111.11111111.11111110 soit **255.255.255.254**.

Enfin, il faut spécifier l'adresse de comparaison : 134.59.137.96, l'adresse paire à cause du fonctionnement du «et logique».

Comparaison entre une sonde Rmon et un Sniffer (type ethereal)

Un Sniffer est surtout un outil d'expertise de réseau. Il permet d'observer les dialogues avec un regard de système expert et détecte les éventuels symptômes qui lui paraissent anormaux afin d'en avertir l'utilisateur. Par exemple, il analyse les délais de réponse d'une station, détaille les dialogues au niveau protocole et en tire les diagnostics. Mais cet outil est également capable d'effectuer une capable de métrologie. C'est pourquoi, un comparatif des possibilités entre Sniffer et Sonde Rmon est indispensable :

Sonde Rmon avec pilotage MeterWare	Sniffer
Capture limitée à 1000 octets ou entête de 500 premiers octets	Capture de trame entière
Environnement graphique et souris	Pas ergonomique, déplacement avec les flèches
Plusieurs captures simultanées avec des filtres différents	Une seule capture possible
Capture max de 1200 trames avec le buffer maximum	Capture au maximum d'environ 23000 trames
Capture de 53 trames si le buffer est de 16384 octets	
Aide en anglais	Aide en français
Affichage structurée des trames en fonction de leur format	Affichage de la trame en brut
Visualisation des trames en même temps que la capture	Choix exclusif entre capture et visualisation
Mesures statistiques très riches	Mesures statistiques limitées
Supervision des stations en temps réel	Pas de supervision des stations
Campagnes de mesure multiples et analyses simultanées	Opération monotâche
Comporte des bugs	Ne comporte pas beaucoup d'anomalies
Génération de trafic sur le réseau	Reste à l'écoute du réseau (trafic généré nul)

L'utilisation intensive des deux types d'équipements fait apparaître non pas une concurrence, mais une complémentarité entre eux. C'est très certainement dommage de monopoliser un Sniffer pour réaliser des observations métrologiques. Il est donc préférable d'agir de manière chronologique : d'une part, on réalise une campagne de mesure avec sonde Rmon et récupération des résultats par

MeterWare, puis on cible l'expertise des dysfonctionnement avec un Sniffer. Mais l'usage du Sniffer est plus délicat car sa maîtrise et l'approfondissement de ses fonctionnalités nécessitent une utilisation importante.

Installation et configuration de la sonde

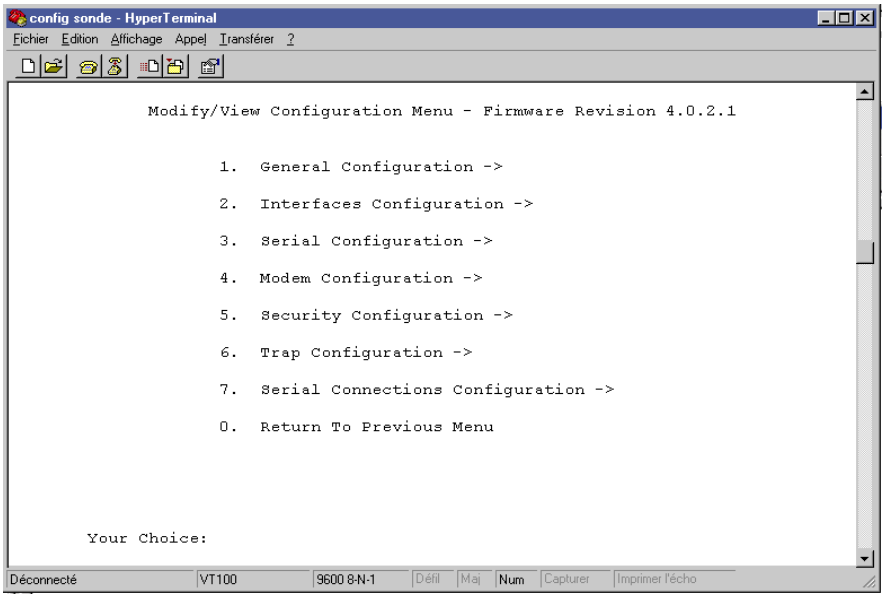
Généralités

La sonde est reliée au PC par un câble "null modem DB9" nécessaire à la configuration de base de la sonde par une session HyperTerminal. La sonde est également reliée au réseau via le HUB 12 ports 10/100BT de la salle de TP, permettant ainsi d'observer le trafic engendré sur un segment par des ordinateurs de type PC, de type Macintosh (AppleTalk et EtherTalk) et par une imprimante laser en réseau. Avant de commencer la manipulation, il est nécessaire de connaître les adresses IP utilisée par le réseau de la salle (et donc à relever)
Vous pouvez aisément vérifier l'adresse IP de votre machine par le menu "*Démarrer/Paramètres/Panneau de Configuration*" puis en cliquant deux fois sur l'icône "*Réseau*". Affichez ensuite l'onglet "*Protocole*", sélectionnez le protocole "*TCP/IP*" et cliquez sur "*Propriétés*". Vous pouvez également vérifier l'adresse Ethernet (adresse MAC) en utilisant « arp –a » dans une fenêtre DOS.

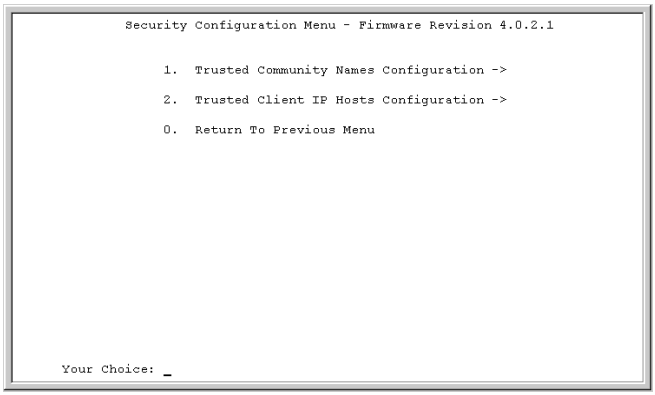
La sonde Rmon2 est reliée à l'ordinateur par un câble série null modem à 9 broches. Si ce n'était pas le cas, cette opération doit être effectuée impérativement avec l'ordinateur et la sonde hors tension. Lancez une session HyperTerminal par le menu "*Démarrer/Programmes/Accessoires/Hyperterminal/HyperTerminal*". Vous devez alors spécifier un nom, choisir l'icône et le port, puis précisez les paramètres de session afin de dialoguer avec la sonde.

- Entrez comme nom "**sonde xxyyyy**" où xx est le jour du TP et yyyy, l'heure du début de la séance,
- Choisissez le premier icône de la sélection,
- Choisissez le port COM1 car la sonde est sur le port série A (COM2 si la sonde est sur le port série B),
- Entrez les paramètres : 9600 bps, moment de 8, aucune parité, 1 bit de stop et aucun contrôle de flux.

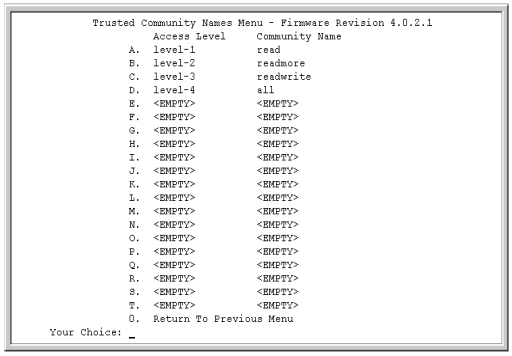
Dans la session, choisissez une émulation **VT100** dans l'onglet "*Configuration*" du menu "*Fichier/Propriétés*". Les autres paramètres (touches de terminal, code ASCII, …) sont corrects.
Mettez maintenant la sonde2 sous tension, les diodes rouges en face avant s'allument. Lorsque ces dernières se mettent à clignoter, appuyez plusieurs fois sur la touche "*Return*" afin de forcer la dialogue avec la sonde2.
Il faut maintenant accéder au menu de configuration en tapant sur "*1*" et en validant.

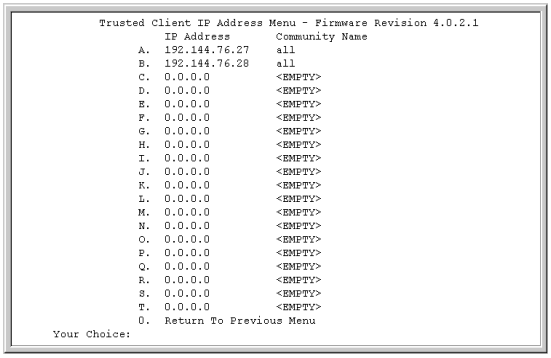


La sonde peut en effet envoyer des requêtes BOOTP pour une machine disposant d'un logiciel de supervision prenant en charge ces requêtes comme Optivity. Si une image de la configuration de la sonde a été enregistrée sur cette machine, la sonde peut alors la télécharger à son démarrage via BOOTFTP. Maintenant, il faut autoriser uniquement les ordinateurs autorisés à accéder à toutes les fonctions et à toutes les données de la sonde et ceci à l'aide du menu "*Security Configuration*". La fenêtre suivante apparaît :

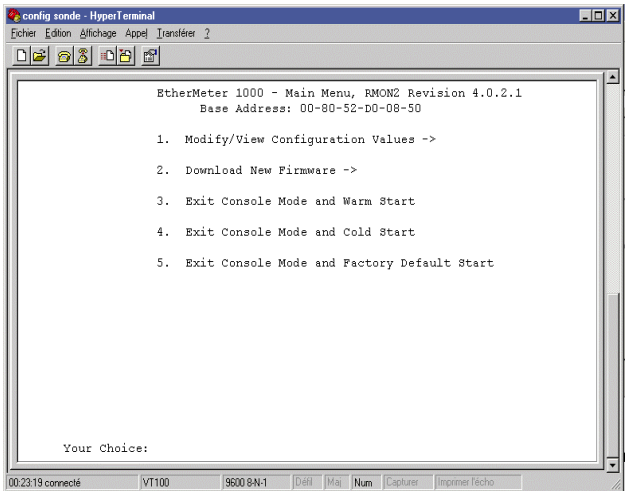

Security Configuration Menu - Firmware Revision 4.0.2.1
1. Trusted Community Names Configuration ->
2. Trusted Client IP Hosts Configuration ->
0. Return To Previous Menu
Your Choice: _

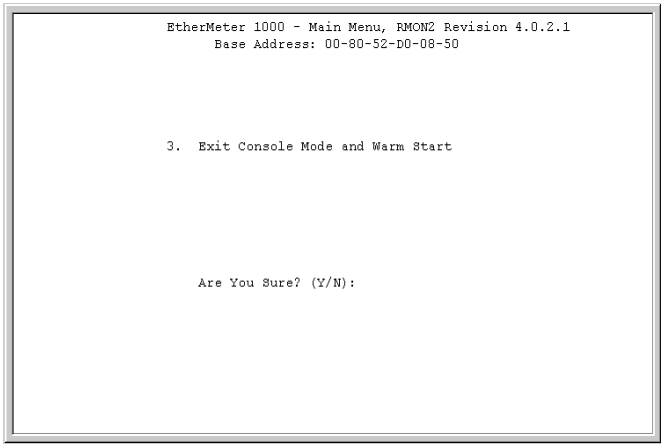
Deux menus sont disponibles. "*Trusted Community Names Configuration*" permet de spécifier des communautés définies par un nom et un niveau de droits d'accès. "*Trusted Client IP Hosts Configuration*" permet de définir à quelle communauté appartient l'utilisateur que vous désirez créer, de définir l'@IP de sa machine et la masque sous-réseau. ATTENTION : si le masque de sous-réseau est 255.255.254.0, il faut entrer 255.255.255.255.



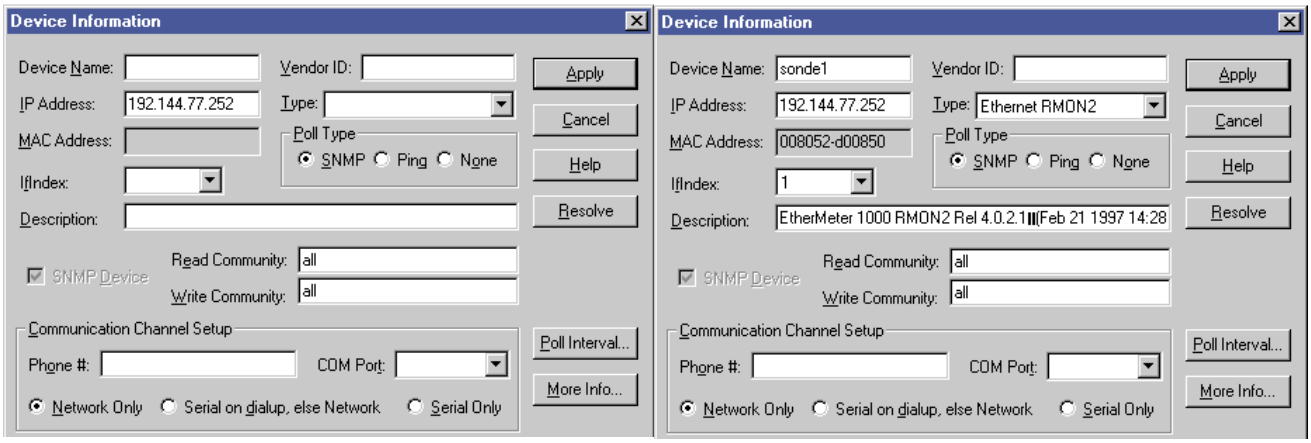


La sonde est configurée, et vous pouvez revenir au premier écran de la session HyperTerminal et effectuez un "***Warm Start***". Confirmez et sur l'écran apparaît "Initialization In Progress …" et les trois diodes rouges en face avant de la sonde doivent se mettre à clignoter. Dès que les diodes arrêtent de clignoter, cela signifie que la sonde a chargé sa nouvelle configuration en mémoire. Eteignez la sonde. Déconnectez-vous de la session HyperTerminal, sauvegardez votre session dans le répertoire temporaire **temp** et fermez la session. Vérifiez que la sonde RMon2 est bien brassée sur le HUB 12 ports 10/100BaseT avec un câble RJ45/RJ45. Remettez sous tension la sonde RMon2. Il est toujours possible si besoin, d'accéder à la sonde via la session HyperTerminal et la liaison série connecté à l'ordinateur maître.

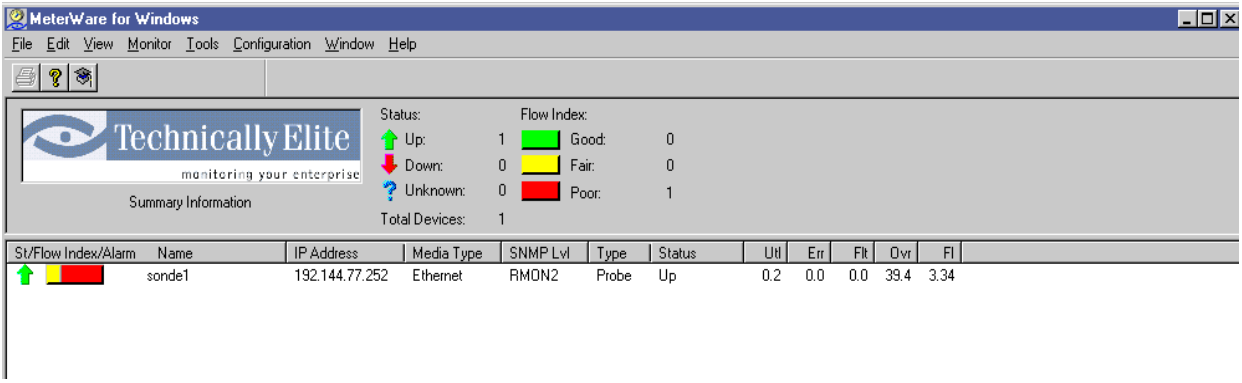

config sonde - HyperTerminal
Fichier Edition Affichage Appel Transférer ?
EtherMeter 1000 - Main Menu, RMON2 Revision 4.0.2.1
Base Address: 00-80-52-D0-08-50
1. Modify/View Configuration Values ->
2. Download New Firmware ->
3. Exit Console Mode and Warm Start
4. Exit Console Mode and Cold Start
5. Exit Console Mode and Factory Default Start
Your Choice:
00:23:19 connecté
VT100
9600 8-N-1


EtherMeter 1000 - Main Menu, RMON2 Revision 4.0.2.1
Base Address: 00-80-52-D0-08-50
3. Exit Console Mode and Warm Start
Are You Sure? (Y/N):

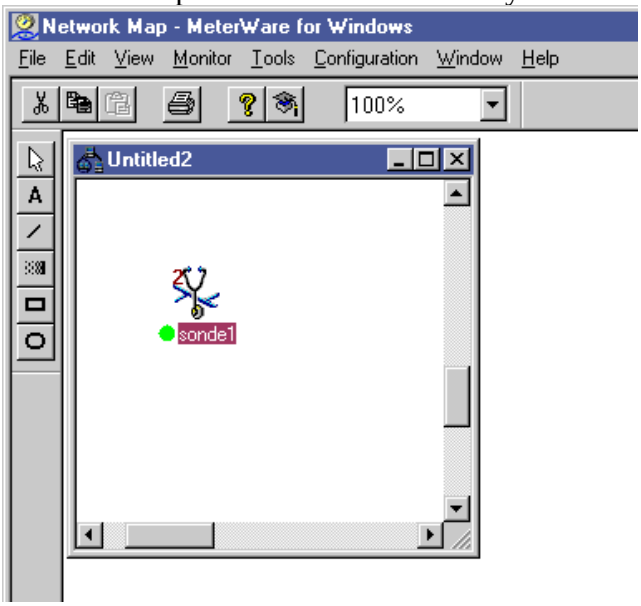
Après avoir démarré le programme Meterware, faîtes apparaître la sonde dans l'interface de MeterWare, lancez "***Edit/New Device***" et remplissez les champs adéquats pour la déclaration de la sonde2 tels que demandé dans l'énoncé du TP et appuyez sur "***Resolve***".



Une requête a été émise sur le réseau pour connaître les informations sur cet équipement. Lorsque l'équipement d'interconnexion est reconnu, cliquez sur "***Apply***" permettant de revenir à l'interface principale. La flèche apparaissant en vert sur le côté gauche signifie que la sonde2 est opérationnelle.



Il est maintenant possible de créer une "Network Map" permettant d'afficher une représentation graphique du réseau et d'utiliser les équipements y figurant. Sélectionnez donc "***View/Map View***". A ce stade de configuration, la sonde2 est prête à être utilisée au moyen des différents services Rmon.



En procédant de la même manière depuis le menu "***Edit/New Device***" et avec les adresses IP appropriées, il vous est possible de visualiser sur votre Network Map, tous les équipements d'interconnexion administrables SNMP sur le segment visualisé (autres sondes, hub, routeur, switch).

Découverte des différents outils de MeterWare

Tout le matériel d'audit de réseau étant installé, il ne reste plus qu'à identifier les outils et les services. En effet, la sonde et le logiciel fonctionnent autour de l'outil Quick View et des services RMON et RMON2 qui représentent les fonctions d'utilisation de la sonde : captures, filtrage, mesure de l'occupation de la bande passante et des erreurs, … Le dialogue est uniquement constitué de requêtes utilisant le protocole SNMP.

L'outil Quick View

Cet outil permet d'obtenir une vue rapide de l'état de santé de son réseau à travers trois observations, en double-cliquant sur l'icône de la sonde2 présente dans la Network Map et en choisissant l'onglet

"***Information***" :
le pourcentage d'utilisation de la bande passante du réseau,

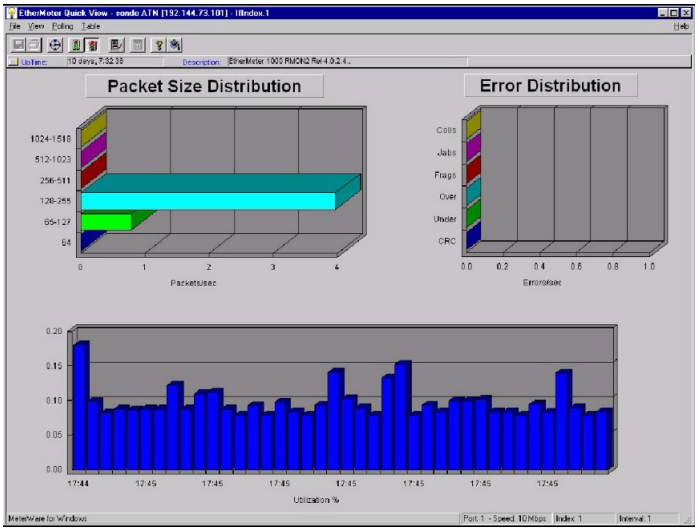
la distribution des paquets par taille,

les éventuelles erreurs rencontrées.

Le menu "**Polling/Sampling Interval…**" permet de définir l'intervalle de temps entre deux consultations de la sonde2. ATTENTION, il faut être conscient du propre trafic généré par les requêtes Quick View. Ci-dessous est fournie une courbe représentant l'occupation de la bande passante par un Quick View en fonction du Polling. Le dialogue avec la sonde2 s'articule autours de deux types de requêtes SNMP :

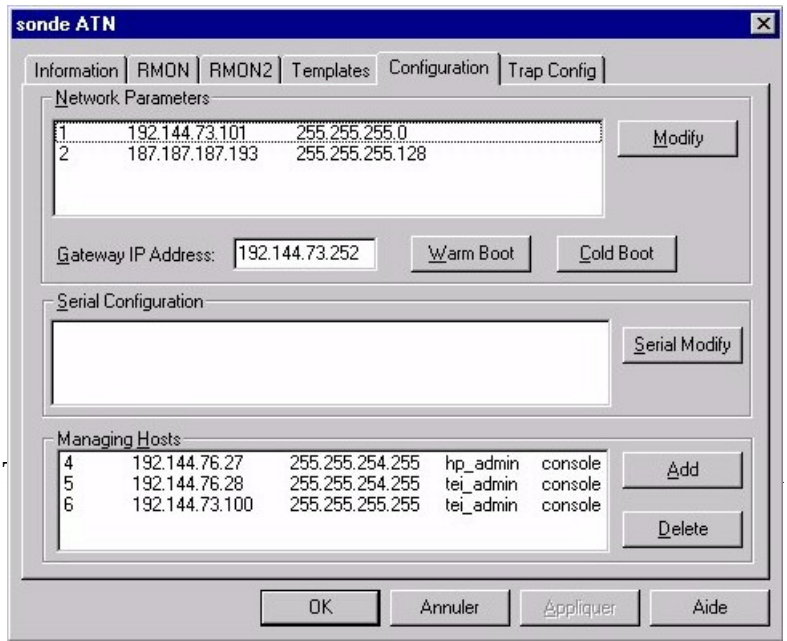
Get-request pour interroger la sonde (d'une taille moyenne de 170 octets),

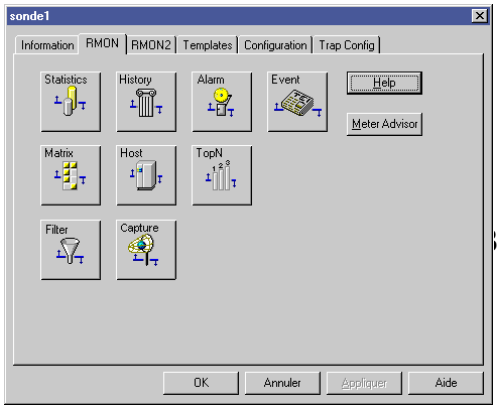
Get-response lorsque la sonde renvoie les compteurs (d'une taille moyenne de 190 octets).



Le service "Configuration"

En cliquant dans la Network Map, sur l'icône de la sonde2 et en sélectionnant le service "***Configuration***", il est possible à la station administration "gtr405p7" d'ajouter ou de supprimer de nouvelles stations d'administration à condition qu'elles soient déclarées avec les droits adéquats. Il est également possible d'établir une table de noms logiques en choisissant "***RMON discovery***" dans le service "***Configuration***" et en sélectionnant l'onglet "***Device***".





Les services Rmon

En cliquant dans la Network sélectionnant le service "***RMON***", une Map, sur l'icône de la sonde2 et en fenêtre apparaît avec un ensemble de rubriques.

Le service Statistics

Il permet d'évaluer les performances du segment surveillé sur cinq points accessibles à partir du menu "***View***" : Utilization, Packet Summary, Size Trend, Error Trend, Packet Table. La taille moyenne des requêtes pour l'utilisation de ce service est de 255 octets pour le Get-request et de 280 octets pour le Get-response :

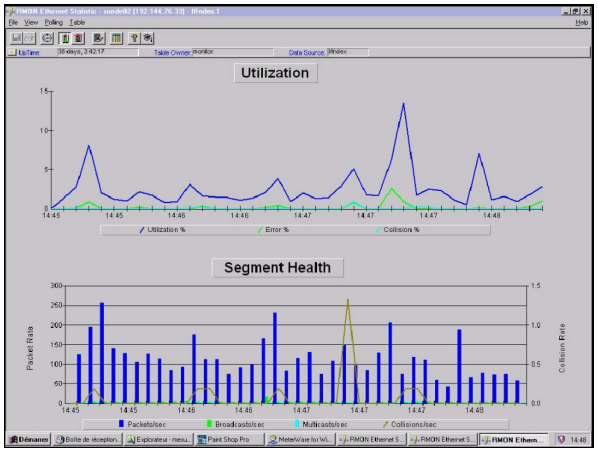
Utilization permet de comparer la charge du réseau avec d'éventuelles erreurs ou rafales de broadcasts,

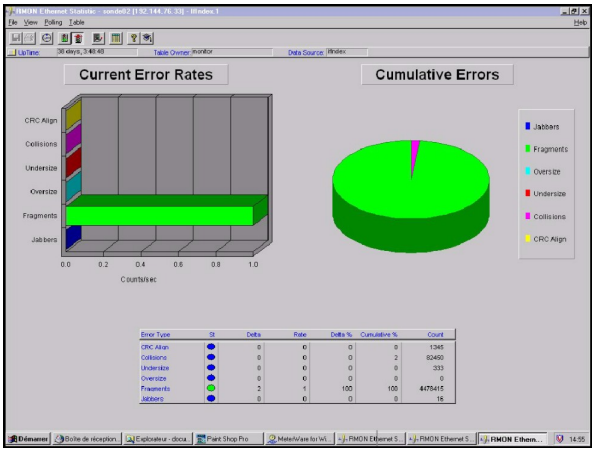
Packet Summary permet de visualiser la distribution des paquets (taille) ainsi que les erreurs survenues,

Size Trend permet de visualiser par taille, différents paquets circulant sur le segment surveillé,

Error Trend permet de visualiser et de différencier les erreurs survenant sur le segment surveillé,

Packet Table offre un récapitulatif de l'activité du réseau sous forme de tableau. Les informations sont comptabilisées en valeur cumulées (Count), sur un intervalle de temps (Delta) ou sur une seconde (Rate).

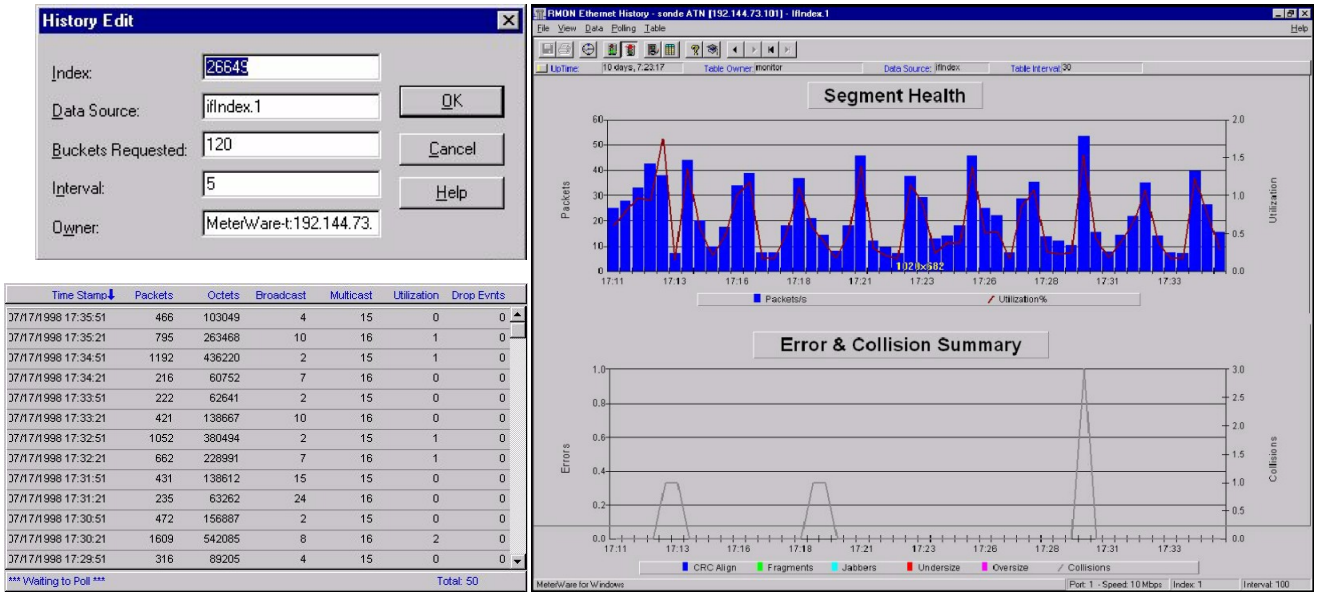




Le service History

Ce service permet de lancer des campagnes de statistiques qui décrivent le comportement du segment surveillé par une représentation graphique du pourcentage d'utilisation de la bande passante, le nombre de paquets par seconde, le pourcentage de collision et d'erreurs par type (CRC

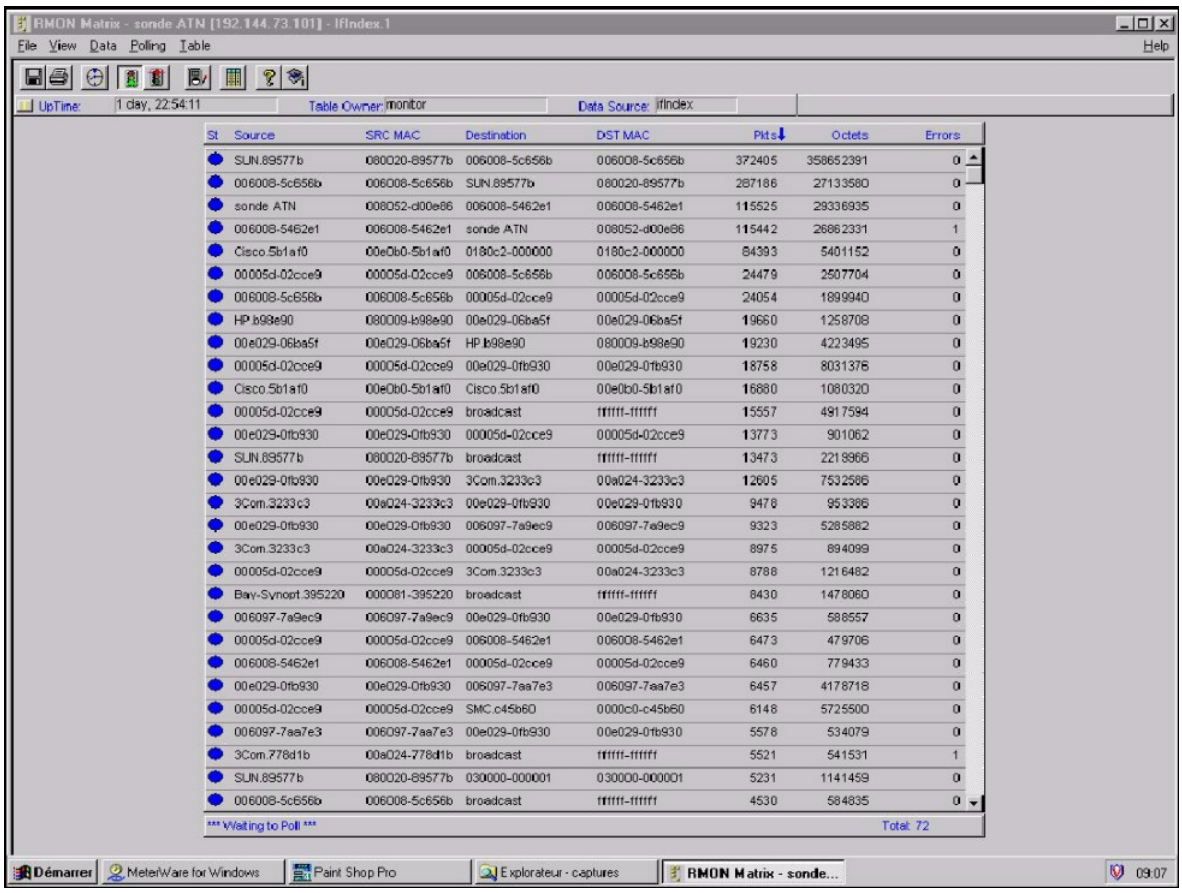
Align, Fragments, Jabber, Undersize, Oversize). Il faut alors préciser le nombre d'échantillons (buckets) et la fréquence d'échantillonnage, ce qui représente en fait la durée de la campagne d'audit. Il est également possible d'affecter une capture à un historique afin d'effectuer du filtrage et donc surveiller le trafic entre des machines particulières. Le rapatriement des historiques utilise environ 1% de la bande passante (255 octets pour le Get-request et 285 octets pour le Get-response). La création du buffer s'effectue par le menu "***Table/Control Table/Index selection/Modify***".



Le service Matrix

Ce service permet d'établir des statistiques sur des dialogues entre équipements du réseau. Chaque ligne du tableau correspond à un échange, dans un sens, d'une machine vers une autre. Pour chaque couple d'équipements, les statistiques comprennent les champs suivants:

- L'état du dialogue entre les deux machines, matérialisé par un indicateur de couleur,
- Le nom de la machine émettrice si le logiciel a pu l'interpoler depuis l'adresse MAC (noms logiques),
- L'adresse MAC de la machine émettrice,
- Le nom de la machine réceptrice si le logiciel a pu l'interpoler depuis l'adresse MAC (noms logiques),
- L'adresse MAC de la machine destinataire,
- Le nombre de paquets émis,
- Le nombre total de bits émis,
- Le nombre d'erreurs.

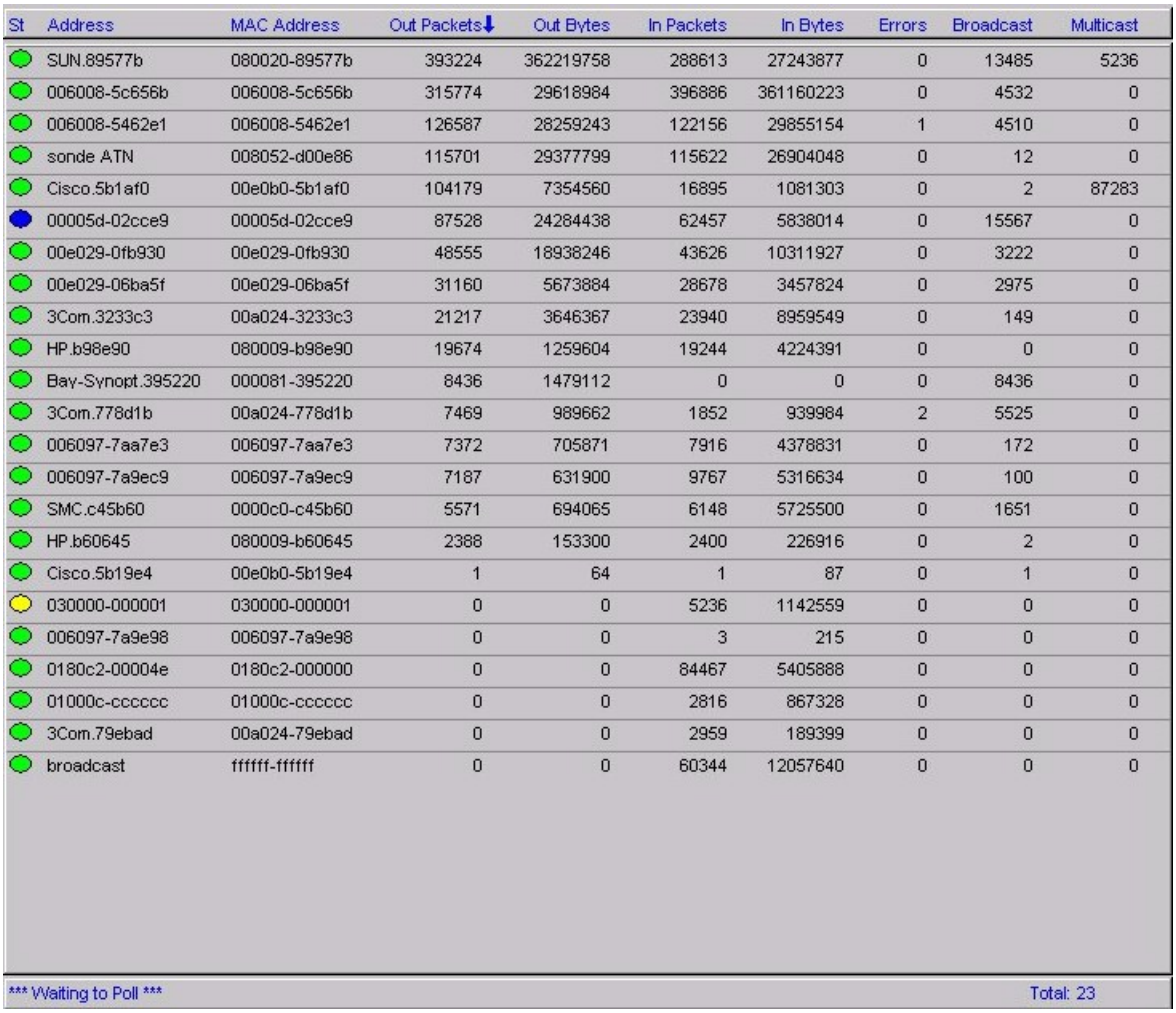


Afin de ne pas surcharger le réseau en utilisant une partie de la bande passante en permanence, il faut choisir un polling supérieur à 40 secondes (Get-request de 250 octets et Get-response de 265 octets).

Le service Host

Ce service permet de connaître quels sont les stations les plus bavardes. En effet, en choisissant une vue cumulative, la sonde donne par ordinateur, les statistiques suivantes :

- L'état du dialogue entre les deux machines, matérialisé par un indicateur de couleur,
- Le nom de la machine émettrice sinon l'adresse MAC,
- Le nom de la machine destinataire sinon l'adresse MAC,
- Le nombre total de paquets et de bits émis,
- Le nombre total de paquets et de bits reçus,
- Le nombre total d'erreurs,
- Le nombre de broadcast et de multicast.



St	Address	MAC Address	Out Packets	Out Bytes	In Packets	In Bytes	Errors	Broadcast	Multicast
	SUN.89577b	080020-89577b	393224	362219758	288613	27243877	0	13485	5236
	006008-5c656b	006008-5c656b	315774	29618984	396886	361160223	0	4532	0
	006008-5462e1	006008-5462e1	126587	28259243	122156	29855154	1	4510	0
	sonde ATN	008052-d00e86	115701	29377799	115622	26904048	0	12	0
	Cisco.5b1af0	00e0b0-5b1af0	104179	7354560	16895	1081303	0	2	87283
	00005d-02cce9	00005d-02cce9	87528	24284438	62457	5838014	0	15567	0
	00e029-0fb930	00e029-0fb930	48555	18938246	43626	10311927	0	3222	0
	00e029-06ba5f	00e029-06ba5f	31160	5673884	28678	3457824	0	2975	0
	3Com.3233c3	00a024-3233c3	21217	3646367	23940	8959549	0	149	0
	HP.b98e90	080009-b98e90	19674	1259604	19244	4224391	0	0	0
	Bay-Synopt.395220	000081-395220	8436	1479112	0	0	0	8436	0
	3Com.778d1b	00a024-778d1b	7469	989662	1852	939984	2	5525	0
	006097-7aa7e3	006097-7aa7e3	7372	705871	7916	4378831	0	172	0
	006097-7a9ec9	006097-7a9ec9	7187	631900	9767	5316634	0	100	0
	SMC.c45b60	0000c0-c45b60	5571	694065	6148	5725500	0	1651	0
	HP.b60645	080009-b60645	2388	153300	2400	226916	0	2	0
	Cisco.5b19e4	00e0b0-5b19e4	1	64	1	87	0	1	0
	030000-000001	030000-000001	0	0	5236	1142559	0	0	0
	006097-7a9e98	006097-7a9e98	0	0	3	215	0	0	0
	0180c2-00004e	0180c2-000000	0	0	84467	5405888	0	0	0
	01000c-cccccc	01000c-cccccc	0	0	2816	867328	0	0	0
	3Com.79ebad	00a024-79ebad	0	0	2959	189399	0	0	0
	broadcast	ffffff-ffffff	0	0	60344	12057640	0	0	0

*** Waiting to Poll *** Total: 23

Etant donné la taille moyenne des requêtes (280 octets pour un Get-request et 300 octets pour un Get-response), le polling doit être supérieur à 15 secondes pour ne pas surcharger la bande passante en permanence avec la trafic généré par le fonction Host.

Le service TopN

Ce service permet de mettre en évidence, les équipements les plus actifs du réseau selon différents critères :

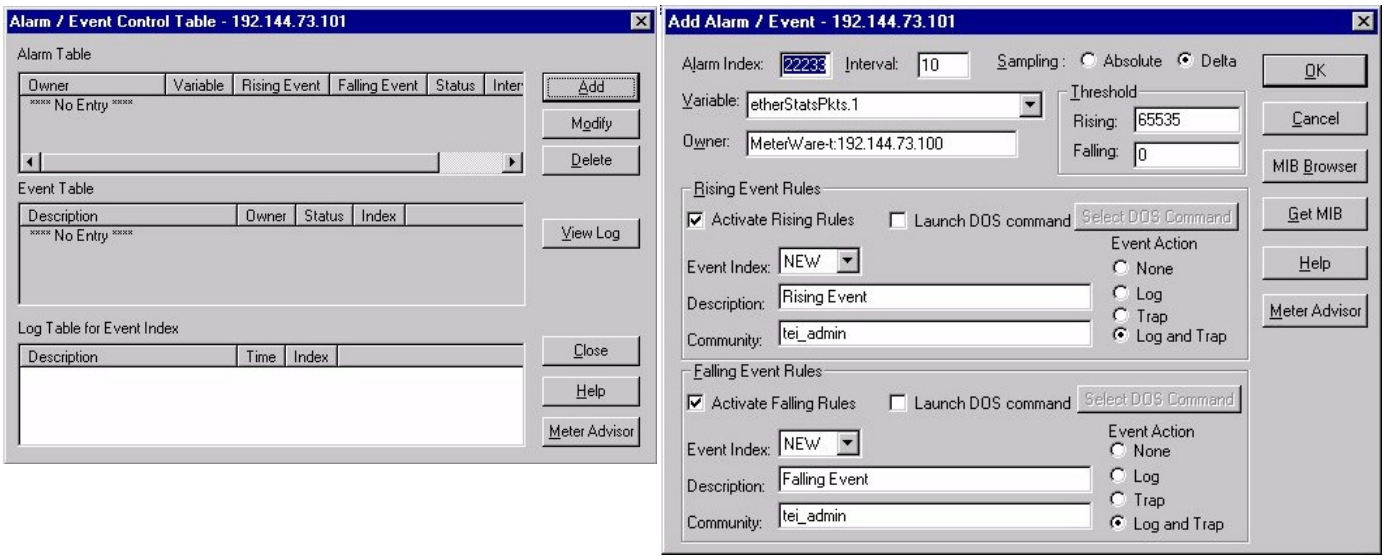
- Les équipements qui émettent le plus ou reçoivent le plus (In packets, Out packets, In octets, Out octets),
- Les équipements générant le plus de broadcast ou de multicast,
- Les équipements générant le plus d'erreurs,

Les services Alarm/Event

Ces services, allant de pair, permettent de manipuler plus précisément les variables de la MIB. Si le réseau est le siège d'un nombre important de broadcast, il est possible d'être averti si le nombre de broadcast par seconde est supérieur au seuil tolérable pour le LAN, sachant qu'une tempête de broadcast peut avoir une durée aléatoire.
Prenons l'exemple suivant : si au bout de 10 secondes, le nombre de broadcast constaté est supérieur à 40 alors il doit y avoir déclenchement d'une alarme vers la sonde2 et vers le journal de bord du MeterWare. La prochaine alarme devra avoir lieu après que le seuil bas soit devenu inférieur à 5

broadcast. Voici la manière de remplir les différents champs :

- Après avoir sélectionné le service "***Alarm***", cliquez sur "***Add***" pour définir l'événement,
- Choisissez dans "***Variable***", l'événement à détecter : **etherStatsBroadcastPkt**,
- Définissez l'intervalle de temps d'observation dans "***Interval***" : **10**,
- Choisissez la méthode d'échantillonnage dans "***Sampling***" : **Delta**,
- Définissez la seuil haut dans "***Threshold/Rising***" : **40**,
- Définissez la seuil haut dans "***Threshold/Falling***" : **5**,
- Sélectionnez "***Log and Trap***" dans les règles d'activation des seuils.



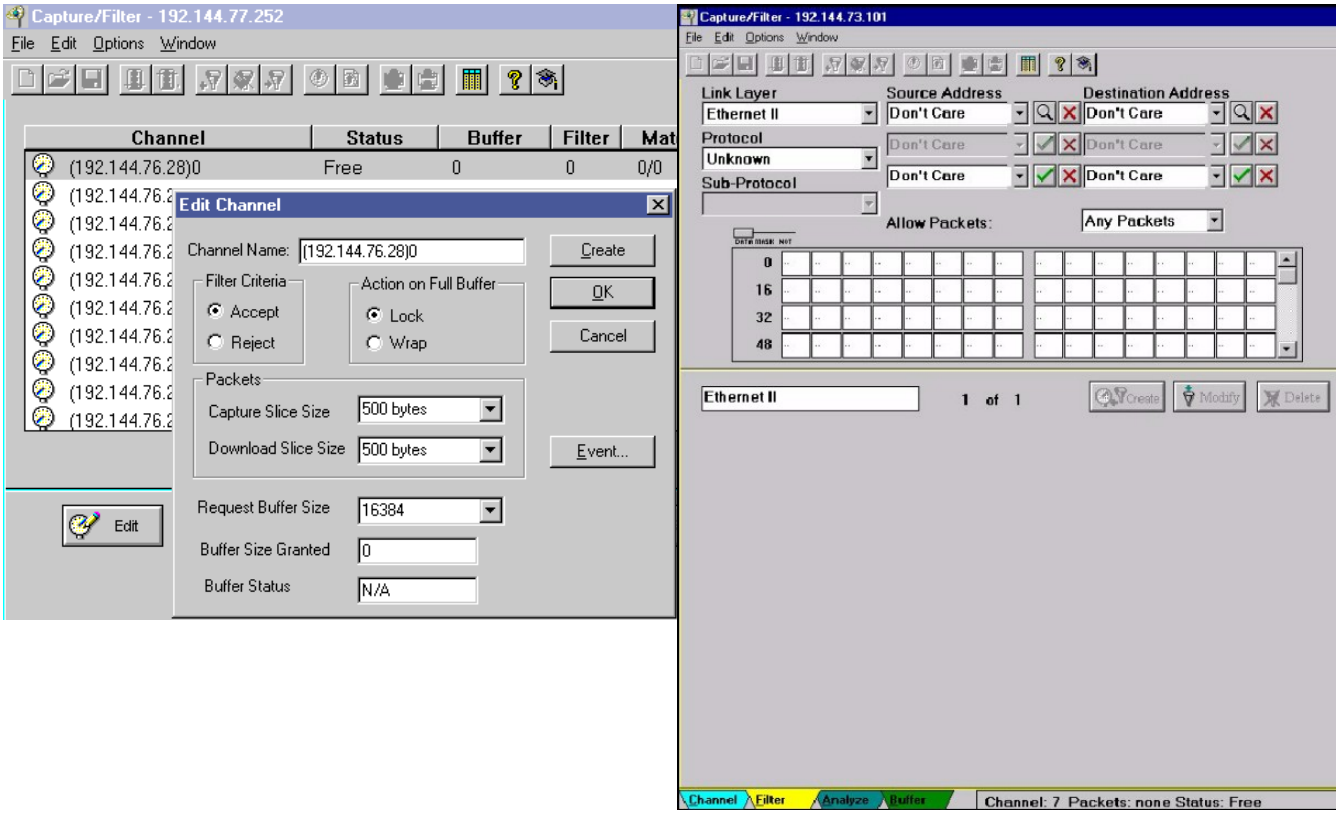
Les services Filter/Capture

Ces services sont certainement ceux qui permettent d'affiner le plus les mesures. Il est certe possible d'effectuer de certains types de paquets et d'en exclure d'autres (capture de toutes les trames émises ou reçues par une machine), mais on peut spécifier le mémoire réservée dans la sonde2 pour stocker les paquets capturés, la taille des paquets que l'on conserve (exprimée en n premiers octets), le fonctionnement de la mémoire (réécriture ou refus des nouveaux paquets lorsque la mémoire est pleine). Les filtres se composent de champs à remplir, représentant les premiers octets d'un paquet (*d'où la nécessité de connaître parfaitement la structure d'une trame TCP/IP*). Il est possible de préciser grâce à une interface graphique, les protocoles, les adresses MAC et IP de source et de destination, à l'instar d'un analyseur de protocoles. Le filtrage peut être défini par le remplissage ou non des conditions paramétrées (accept ou reject). Le rapatriement de ces captures utilise en moyenne 0.025% de la bande passante, la taille moyenne des requêtes étant de 290 octets pour les Get-request et 320 octets pour les Get-response.

La première étape de la création d'une capture est de lui allouer un "***channel***" sur la sonde2, c'est-à-dire un endroit où seront stockées toutes les données inhérentes à la capture. Pour cela, il faut définir les propriétés en cliquant sur "***Edit***". Les options sont alors les suivantes :

Channel Name : nom de la capture,
Filter Critéria : indique si le paquet correspondant aux critères doit être accepté ou refusé,
Action on full buffer : le buffer plein doit être bloqué (Lock) ou recyclable (Wrap),
Capture Slice Size : définition de la taille du paquet qui sera capturé par la sonde2,
Dowload Slice Size : définition de la taille du paquet qui sera envoyé à MeterWare par la sonde2,
Request Buffer Size : taille (en octets) réservée sur la sonde2 pour les données de la capture,
Buffer Size Granted : taille du buffer en octets, accordée pou la capture,
Buffer Status : N/A (état non déterminé) – Avail (buffer pour la capture créé) – Full

(buffer plein).

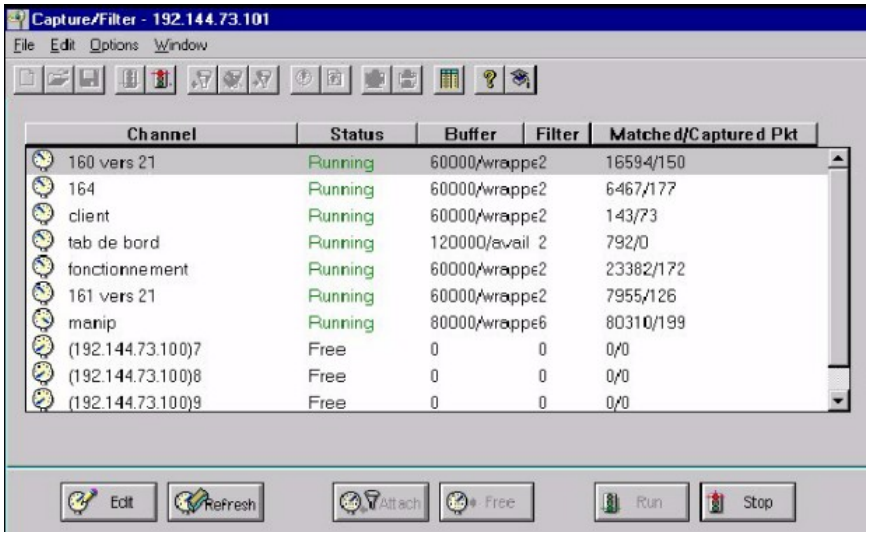


Une fois les différents choix effectués, la validation s'effectue en cliquant sur "***Create***". Il faut toutefois rester conscient qu'un buffer ou une taille de paquet mal ajustée peut immobiliser la sonde2 en monopolisant ou rendre la capture inutile.
En cliquant sur le second onglet "***Filter***", il est possible de définir les filtres en choisissant les protocoles, les adresses IP et MAC de destination et source, les erreurs (CRC, Jabber, …) et même un élément dans le paquet. Toutes ces données pouvant être combinées, il existe donc une très large gamme de possibilités de filtres. Pour cela; il faut cliquer sur "***Create***" et remplir les champs :

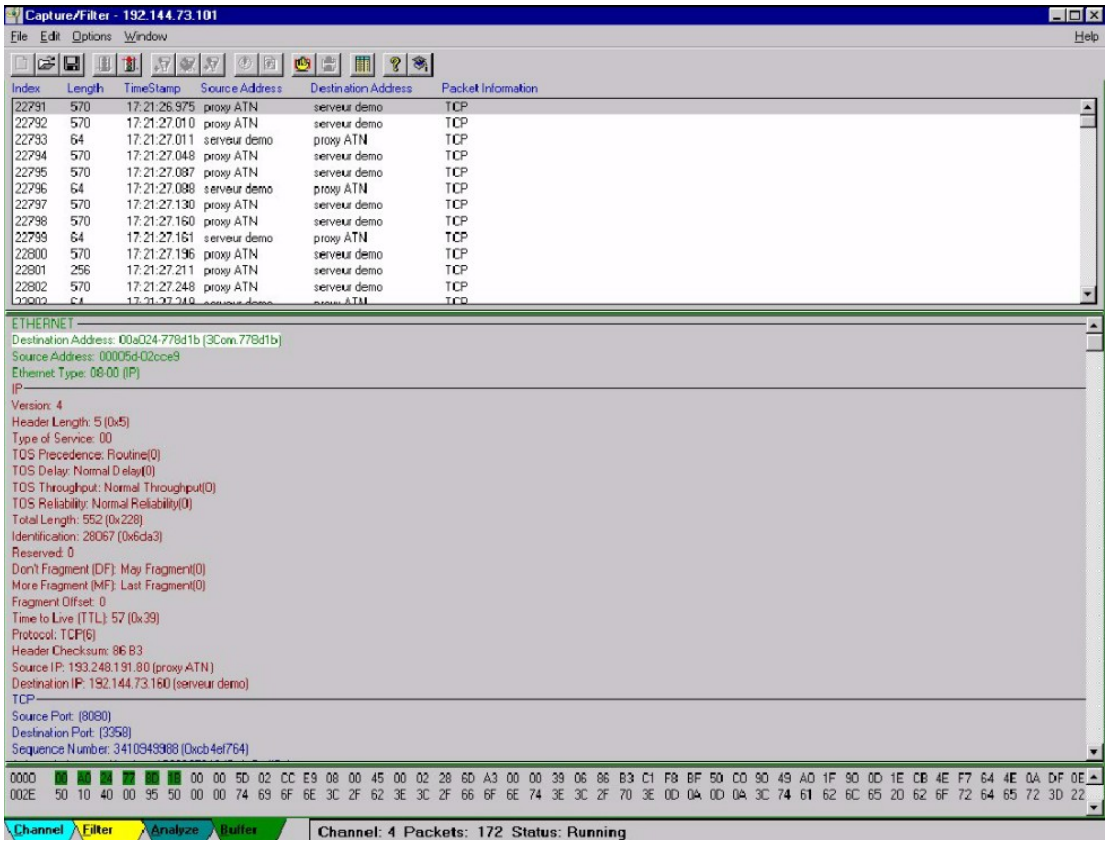
Link Layer : choix du type d'encapsulation au niveau liaison de données,
Protocol : sélection du protocole,
Sub-Protocol : sélection de protocole de couche supérieure,
Allows Packets : permet le filtrage sur certains paquets (selon le type d'erreurs),

---

Les changements effectués sont alors pris en compte en cliquant sur "*Modify*". Pour créer un autre filtre sur le même "channel", il faut réitérer la procédure depuis "Create". La capture est lancée est cliquant "***Run***" et arrêtée en cliquant sur "***Stop***".



Il est alors possible de visualiser les paquets capturés en cliquant sur l'onglet "***Buffer***" qui permet de rapatrier les paquets du buffer de la sonde et de les décoder par couche jusqu'à la couche 4 des protocoles.


Capture/Filter - 192.144.73.101
File Edit Options Window
Help
Index Length TimeStamp Source Address Destination Address Packet Information
22791 570 17:21:26.975 proxy ATN serveur demo TCP
22792 570 17:21:27.010 proxy ATN serveur demo TCP
22793 64 17:21:27.011 serveur demo proxy ATN TCP
22794 570 17:21:27.048 proxy ATN serveur demo TCP
22795 570 17:21:27.087 proxy ATN serveur demo TCP
22796 64 17:21:27.088 serveur demo proxy ATN TCP
22797 570 17:21:27.130 proxy ATN serveur demo TCP
22798 570 17:21:27.160 proxy ATN serveur demo TCP
22799 64 17:21:27.161 serveur demo proxy ATN TCP
22800 570 17:21:27.196 proxy ATN serveur demo TCP
22801 256 17:21:27.211 proxy ATN serveur demo TCP
22802 570 17:21:27.248 proxy ATN serveur demo TCP
ETHERNET
Destination Address: 00a024-778d1b (3Com 778d1b)
Source Address: 00005d-02cce9
Ethernet Type: 08-00 (IP)
IP
Version: 4
Header Length: 5 (0x5)
Type of Service: 00
TOS Precedence: Routine(0)
TOS Delay: Normal Delay(0)
TOS Throughput: Normal Throughput(0)
TOS Reliability: Normal Reliability(0)
Total Length: 552 (0x228)
Identification: 28067 (0x6da3)
Reserved: 0
Don't Fragment (DF): May Fragment(0)
More Fragment (MF): Last Fragment(0)
Fragment Offset: 0
Time to Live (TTL): 57 (0x39)
Protocol: TCP(6)
Header Checksum: 86 B3
Source IP: 193.248.191.80 (proxy ATN)
Destination IP: 192.144.73.160 (serveur demo)
TCP
Source Port: (8080)
Destination Port: (3358)
Sequence Number: 3410949988 (0xcb4ef764)
0000 00 00 00 00 00 00 00 00 00 00 5D 02 CC E9 08 00 45 00 02 28 6D A3 00 00 39 06 86 B3 C1 F8 BF 50 C0 90 49 A0 1F 90 0D 1E CB 4E F7 64 4E 0A DF 0E
002E 50 10 40 00 95 50 00 00 74 69 6F 6E 3C 2F 62 3E 3C 2F 66 6F 6E 74 3E 3C 2F 70 3E 0D 0A 0D 0A 3C 74 61 62 6C 65 20 62 6F 72 64 65 72 3D 22
Channel Filter Analyze Buffer
Channel: 4 Packets: 172 Status: Running

A partir de cet écran, il est possible de sauvegarder les résultats sous un format .txt qu'il est possible d'importer sous Excel. Enfin, l'onglet "***Analyse***" permet d'affiner une analyse en portant des filtres sur des paquets déjà capturés. Dans l'**Annexe2** figurent la manière de créer un historique avec filtrage, des précisions sur le service Matrix et des réponses à quelques problèmes que vous pourriez rencontrer. D'autres services sont proposés comme étant des extensions aux services de base RMON : il s'agit des services **RMON2**. Parmi ceux-ci :

- **NND** : détecte les nouveaux équipements connectés sur le LAN et non identifiés dans la table des hosts,
- **IPMap** : repère les correspondances @MAC/@IP permettant de détecter les duplications d'@IP,
- **Peak** : analyse les pics en terme de nombre de trames/erreurs/broadcast par seconde,
- **Top10** : visualise les plus bavards au niveau MAC, IP, broadcast et les dialogues gourmands en BP,
- **Zoom** : permet en un écran, une synthèse des statistiques fournies par la sonde avec :
  - répartition des paquets par taille
  - répartition des protocoles
  - répartition des erreurs
- **Protocol** : fournit les protocoles les plus utilisés sur le LAN.

Bien qu'offrant de nombreuses possibilités, il n'est pas possible avec la sonde 1000e de lancer plus de dix captures simultanément, et ce même s'il reste encore de la mémoire disponible dans la sonde. Il n'est pas possible non plus d'attribuer un nom aux historiques ne facilitant pas leur repérage lorsqu'il en existe plusieurs avec le même nombre d'échantillons et la même durée. La seule manière de sauvegarder un historique est sous forme de fichier texte. Cependant, dans cette sauvegarde, le logiciel arrondi les mesures à l'entier supérieur ce qui annule par exemple les valeurs de bande passante inférieur à 1%, ce qui peut être très génant.

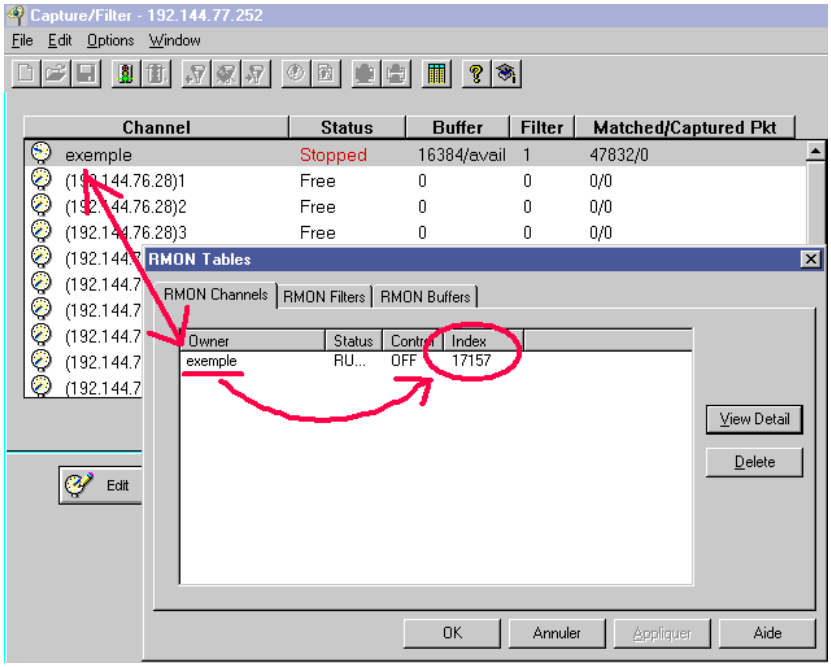
Fiche technique de la sonde Ethermeter 1000e de J3TEL

Hardware	Processor : Intel i960CF, 25 MHz, 50 MIPS
LAN interface	Both interfaces come standard IEEE 802.3 RJ-45 Token Ring IEEE 802.3 DB9 Connector
Serial interface	Asynchronous RS-232, up to 38.4 Kbps
Dimensions	Single-Unit Enclosure : Lenght : 36cm / 14 in Height : 4.2cm / 1.6 in Width : 22cm / 8.6 in
Power	110/240 volts, 50/60 Hz, 1.6A, 65 Watts
Environment	Operating temperature : 0-50 degrees C, 32-122 degrees F Humidity : UP to 95% (non-condensing) Safety : CSA approved Emissions : Fcc Class A
System configuration	A single-height enclosure or Card with an Intel 25 MHz i960CF microprocessor, options of 2MB, 4MB 8MB, 16MB or 32MB of DRAM, 512kB of flash

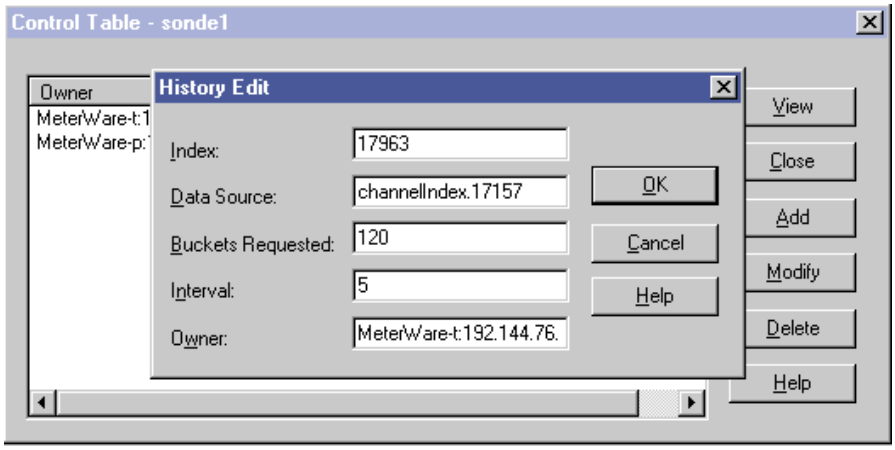
	memory and 32kB of non-volatile flash and a Token Ring controller.
Options	1000e is the enclosure model 1000c is a card that plugs into any standard ISA PC slot Configurations with 4MB or more recommended for Applications requiring extended packet captures or Multiple host, matrix and history tables.
Compliance	All unit comply with all released RMON Standards.

MeterWare - Création d'un historique avec filtrage

Il faut réaliser la partie filtrage telle que définie dans la manipulation et en précisant, lors du la création du channel, "***Wrap***" dans "***Action on Full Buffer***". Ensuite, "***RMON Tables***" doit être sélectionné dans le menu "***Window***" et il faut noter le numéro d'index correspondant au channel créé :



Maintenant il faut créer avec le service "***History***" l'historique à partir de "***Tables/Control Tables***"

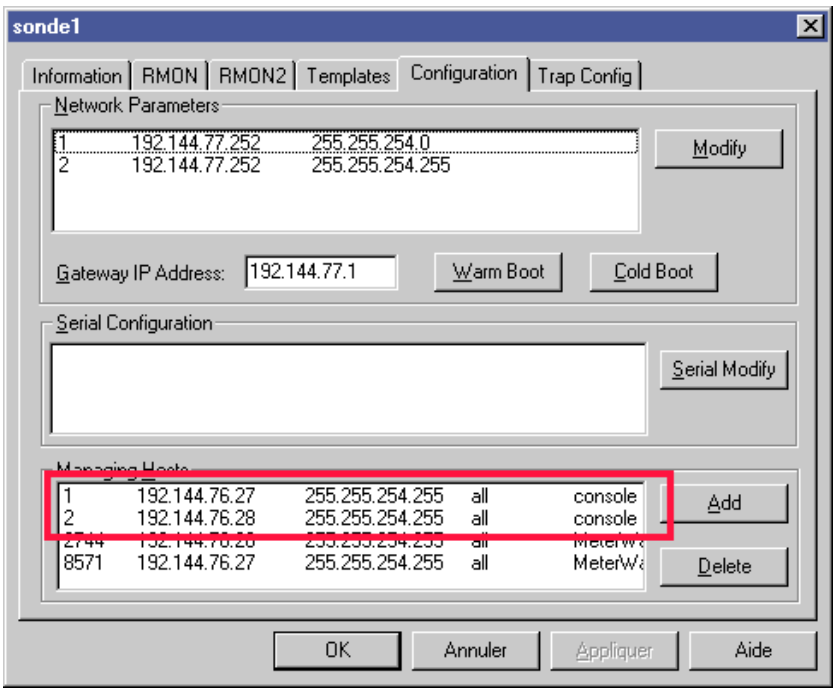


- Choisir "Add" pour rajouter une table.
- Dans "Data Source", tapez «channelIndex.» puis le numéro du channel créé.
- Dans "Buckets Requested", précisez le nombre d'échantillons dont vous avez besoin.
- Dans "Interval", précisez la durée de chaque échantillon (en secondes).
- Le produit de ces deux paramètres vous indique la durée de votre historique (en secondes).
- Enfin cliquez sur "OK" puis sur "View".

MeterWare - Quelques problèmes classiques d'utilisation

Vous n'arrivez pas à écrire dans la sonde, à créer une capture ou établir un historique

Vous n'avez peut-être pas les droits suffisants pour effectuer ces opérations. Pour vérifier vos droits, cliquez sur la sonde et sélectionnez l'onglet "***Configuration***" :



Dans "***Managing Hosts***" vérifiez que vous avez une ligne "***console***" avec votre adresse IP et le nom de la communauté de niveau 4. Si cette ligne n'apparaît pas, dommage... Vous devez reprendre la configuration de votre sonde et bien spécifiez une communauté de niveau 4 avec votre adresse IP y appartenant.

Votre historique avec filtrage ne tient pas compte des filtres

Vérifiez que vous avez bien lancé la capture associée (en cliquant sur "***Run***") et que le numéro d'index soit le bon.
Vérifiez que vous avez bien mis un point entre "channelIndex" et le numéro d'index.
Respectez scrupuleusement la case définie par la documentation (**channelIndex** et pas **Channelindex**).

Glossaire

Adresse IP : C'est le système d'adressage qui permet au protocole Ethernet d'identifier une machine. Une adresse IP est composée de 12 chiffres décimaux sous la forme xxx.xxx.xxx.xxx, Par exemple, 134.59.137.102. Les adresses IP sont rangées suivant différentes classes A, B et C, chacune répondant au besoin d'un certain nombre de connexion.

Adresse MAC : L'adresse MAC est définie par le constructeur d'équipement réseau. Elle se compose de 6 octets. Elle se présente sous la forme xxxxxx-xxxxxx. Les trois premiers octets dépendent du constructeur. Par exemple, 080020 pour SUN et 02608c pour 3Com.

Agent SNMP : Agent implémenté par la plupart des constructeurs d'équipements administrables permettant de conserver des données relatives à l'état des interfaces réseaux, aux trafics entrants et sortants, aux erreurs détectées sur le support de transmission (le média).

Alignment : Une trame désalignée est une trame dont le nombre de bits n'est pas un multiple de huit. La structure de la trame ne représente plus une suite d'octets entier. Cet erreur entraîne une erreur CRC.

Bandwith : (Bande passante) Capacité d'un canal de transmission, mesurée en bits par seconde (bps). La bande passante d'un réseau Ethernet est de 10 Mbps.

BOOTP : Le protocole BOOTP permet d'attribuer automatiquement une adresse IP à une adresse MAC chaque fois qu'un appareil est démarré. De plus, il peut également définir le masque de sous-réseau et la passerelle par défaut.

Broadcast : (diffusion) Paquet émis par une machine à destination de toutes les autres machines du réseau.

Broadcast storm : Broadcasts multiples, qui peuvent être la cause de pannes de réseau car ils absorbent souvent toute la bande passante disponible.

Buffer : Espace mémoire allouable de façon temporaire dans un équipement afin d'y stocker des données.

Cascade segments : (segments en cascade) Segments qui parcourent la pile de haut en bas par les câbles de cascade, auxquels les segments internes du PS Hub 40 se raccordent (ou desquels ils s'isolent).

Collision : Erreur typique d'un réseau Ethernet due à l'émission simultanée de deux paquets.

Console port : (Port de console) Le port série du PS Hub 40 qui permet de relier un terminal ou un modem. La plupart du temps, il est utilisé pour l'administration locale. The port on the PS Hub 40 accepting a terminal or modem connector.

CRC : Cyclic Redondant Code. Le CRC est un moyen de contrôler la validité d'un paquet transmis sur le réseau. Le CRC calculé à partir des bits du paquet, est recalculé à la réception. S'il n'y a pas concordance, le paquet a été corrompu.

Ethernet : Spécification de réseau local (LAN) développé conjointement par Xerox, Intel et Digital

Equipment Corporation (DEC). Ethernet fonctionne à 10 Mbps et utilise CSMA/CD (Carrier Sense Multiple Access / Collision Detection) pour les transmissions câblées.
Fragment : Trame trop courte (inférieure à 64 octets) et comportant une erreur de CRC.

Hub : Equipement d'interconnexion dont la tâche est de lier plusieurs machines entre elles au sein d'un réseau Ethernet. Un Hub se charge de régénérer le signal, mais il détecte également les erreurs de CRC, les collisions ou les jabbers. Il peut s'agir d'un équipement dit intelligent, administrable à distance par des requêtes SNMP. En contrepartie, un Hub génère un temps de traversée qui augmente le RTD.

IPX : Internetwork Packet Exchange (Echange de paquets inter-réseaux). Protocole utilisé dans les réseaux Netware.

Jabber : Ce type d'erreur se produit lorsqu'un équipement réseau se bloque en émission. Cela est matérialisé par une trame trop longue (supérieure à 1518 octets) et comportant une erreur de CRC.

LAN : Local Area Network (réseau local). Un réseau de ressources informatiques (stations de travail, imprimantes, serveurs, etc) connectées sur une zone géographique relativement petite (habituellement, un étage, voire un bâtiment). Caractérisé par un haut débit et de faibles taux d'erreurs.

Load balancing : (Equilibrage de charge) Consiste à regrouper les utilisateurs en segments d'utilsateurs qui communiquent souvent entre eux. L'objectif est d'équilibrer l'utilisation du réseau sur les différents segments en fonction de leur bande passante.

MIB : Management Information Base (base d'information d'administration). Contient les informations d'administration et les paramètres d'un appareil. Les MIBs sont accessibles par Simple Network Management Protocol (SNMP) pour stocker les attributs des systèmes administrés. Le PS Hub 40 contient son propre MIB interne.

Multicast : Copie de paquets uniques vers un ensemble spécifique d'adresses réseau. Ces adresses sont spécifiées dans le champ « adresse de destination » du paquet.
Oversize : Trame trop longue (supérieur à 1518 octets) sans erreur de CRC.

Protocole : Ensemble de règles de communication entre appareils d'un réseau. Ces règles décrivent le format, les délais, l'enchaînement et le contrôle d'erreurs.

Répartiteur de distribution : Nœud de concentration des câbles vers les points d'accès situés dans les salles.

Rmon : Remote Monitoring (surveillance à distance). Sous-ensemble de SNMP MIB II qui permet de surveiller et d'administrer un appareil avec jusqu'à dix groupes de paramètres différents.

Rocade : Câbles reliant les répartiteurs de distribution deux à deux.

Transceiver : Equipement permettant l'interconnexion entre deux médias différents.

RTD : Rond Trip Delay, temps que met une trame Ethernet pour traverser de bout en bout le réseau. Plus ce temps est long et plus les risques de collisions sont importants.

Segment : branche d'un réseau Ethernet.

SLIP : Serial Line Internet Protocol (protocole Internet pour ligne série). Un protocole qui permet de transmettre des paquets IP sur une connexion série.

SmartAgent : (Agent intelligent) Agents d'administration intelligents contenus dans les appareils et systèmes de connectivité logiques, qui réduisent la charge de travail d'une station de gestion de réseau et qui réduisent le trafic lié à l'administration du réseau.

SNMP : Simple Network Management Protocol (protocole simple de gestion de réseau). Protocole destiné initialement à gérer les réseaux internets bâtis sur TCP/IP. Actuellement implémenté sur une grande variété de stations et d'équipements réseau, il peut être utilisé pour gérer divers aspects du réseau et du fonctionnement des clients.

Stack : (pile) Groupe de hubs connectés entre eux de façon à fonctionner comme un simple répéteur logique.

Switch : Equipement de segmentation de réseau dont le rôle principal est de gérer la transmission de paquets au travers des différents segments. Contrairement au Hub, les temps de traversée sont négligeables.

Telnet : Protocole applicatif qui s'appuie sur TCP/IP, fournissant un service de terminal virtuel qui permet de se connecter à des ordinateurs distants et de les utiliser comme si l'utilisateur utilisait directement ces ordinateurs.

UDP : User Datagram Protocol. Protocole standard de l'Internet qui permet à une application de transmettre un datagramme à une autre application sur un autre appareil.

Undersize : Trame trop courte (inférieur à 64 octets) sans erreur de CRC.

VT100 : Catégorie de terminaux qui utilisent les caractères ASCII. Les écrans VT100 affichent les informations en mode texte.